Colegiul Medicilor din România

GHIDUL MEDICULUI

PENTRU PROTECȚIA DATELOR CU CARACTER PERSONAL

www.gdpr.cmr.ro

GHIDUL MEDICULUI

PENTRU PROTECȚIA DATELOR CU CARACTER PERSONAL

www.gdpr.cmr.ro

Colegiul Medicilor din România

Descrierea CIP a Bibliotecii Naționale a României

COLEGIUL MEDICILOR DIN ROMÂNIA
Ghidul medicului pentru protecția datelor cu caracter personal -
București, 2023

ISBN 978-630-6131-27-5

Autori: **Anamaria Nițulescu, Nicolae Ploeșteanu, Dan Ioan Gurghian, Darius Fărcaș**
Tehnoredactor și designer grafic**: Camelia Gurghian**
Colaborator tehnic: **GDPR Complet**

www.gdpr.cmr.ro
www.cmr.ro

CUPRINS

PARTEA I | CAPITOLUL 1

CUVÂNT INTRODUCTIV

Colegiul Medicilor din România

GHID DEZVOLTAT DE

ÎN COLABORARE CU GDPRComplet.ro

Stimate colege și stimați colegi,

În numele echipei care a contribuit la realizarea acestui Ghid, vă mulțumesc pentru interesul dumneavoastră. Considerăm acest material nu doar util, ci esențial pentru armonizarea practicilor de protecție a datelor în sistemul medical românesc. Datele medicale reprezintă, fără îndoială, unele dintre cele mai sensibile informații cu care lucrăm. Este imperativ ca fiecare dintre noi - ca profesionist în sănătate - să își actualizeze constant cunoștințele și să respecte reglementările existente, pentru a asigura confidențialitatea acestor date.

Ghidul pe care îl aveți în față se bazează pe un cadru legislativ riguros. Acesta include prevederile Regulamentului General privind Protecția Datelor (RGPD), dar și orientări provenite de la organisme internaționale, exemple de amenzi aplicate, practici din alte țări, și așa mai departe. Materialul urmărește să fie atât practic, cât și ușor de înțeles. Scopul său este de a ne ajuta să ne conformăm legilor actuale și să minimizăm riscurile legate de gestionarea datelor medicale sensibile.

Vă încurajăm să folosiți acest Ghid ca pe o resursă, cu scopul îmbunătățirii practicilor actuale și al consolidării unei culturi a protecției datelor, văzută ca o componentă intrinsecă a calității asistenței medicale. Nu putem subestima legătura strânsă dintre etica medicală, aspectele juridice și gestionarea datelor pacienților. Aceste componente sunt pilonii pe care se construiește o practică medicală responsabilă și etică.

Fiecare medic are o răspundere profundă în a proteja datele pacienților săi, nu doar ca o cerință legală, ci și ca un fundament al încrederii și respectului reciproc. Ca medici, noi avem, de asemenea, o poziție privilegiată, respectiv aceea de a fi lideri în promovarea unei astfel de culturi, indiferent de rolul nostru în cadrul echipei sau unității medicale și în orice tip de context organizațional care impune comportamentul nostru responsabil privind protecția datelor.

Vă invităm să vă alăturați efortului colectiv de a instaura o cultură a protecției datelor în sistemul medical românesc. Aceasta este o misiune care ne implică pe toți.

Sperăm că acest Ghid va fi un instrument valoros în activitatea dumneavoastră zilnică. Așteptăm cu interes opinii și sugestii de completare sau de îmbunătățire pe platforma noastră dedicată: www.gdpr.cmr.ro.

Cu deosebită considerație,
Prof. Univ. Dr. Daniel Coriu
Președinte
Colegiul Medicilor din România

Prezentul Ghid a fost realizat de Colegiul Medicilor din România în cadrul unui proiect derulat în perioada ianuarie - septembrie 2023, cu implicarea membrilor Biroului Executiv, respectiv: prof. univ. dr. Daniel Coriu (Președinte), dr. Gheorghe Borcean (Vicepreședinte), dr. Călin Bumbuluț (Vicepreședinte), dr. Valeria Herdea (Vicepreședinte), șef de lucrări dr. Gindrovel Dumitra (Secretar General).

Forma tipărită a Ghidului însoțește formatul digital disponibil pe platforma: www.gdpr.cmr.ro.

Pentru a oferi medicilor din România un instrument de lucru accesibil, aplicabil și adaptabil nevoilor profesiei medicale, formatul digital al Ghidului va fi actualizat în timp real, în acord cu viitoare modificări legislative relevante și/sau cu evoluția cazuisticii specifice domeniului medical.

Forma tipărită a Ghidului va fi de asemenea actualizată periodic, după cum va fi necesar, pentru a asigura concordanța cu formatul digital.

Mulțumim totodată membrilor Consiliului Național al Colegiului Medicilor din România pentru susținerea proiectului care dezvoltă platforma www.gdpr.cmr.ro și, implicit, pentru contribuția la realizarea acestui Ghid, respectiv: dr. Olimpiu Florin Achim, dr. Mugurel Stene Andronache, dr. Cristina-Daniela Atănăsoaie-Iacob, dr. Andrei Romică Baciu, dr. Roxana Maria Mitruța Balaci, dr. Teodora Andia Banu Bradu, dr. Ana Băleanu, dr. Valentin George Bănică, dr. Constantin Cârstea, prof. univ. dr. Emanoil Ceaușu, dr. Roxana-Florentina Chivu, dr. Laura Liliana Ciuntu, dr. Ioan Dănuț Cocoi, șef de lucrări dr. Adrian-Vasile Comănici, dr. Ioan Cordea, șef de lucrări dr. Daniel Costache, dr. Gabriela Georgeta Dascăl, dr. Adrian Dărăbanțiu, dr. Manuela Dăscălescu, dr. George Adrian Enculesei, dr. Elena-Anca Francisc, dr. Marian Gherghiță, dr. Ioan-Răzvan Grecu, dr. Lucica Irina Grigorașcu, prof. univ. dr. Octavian Fulger Lazăr, dr. Claudia Iulia Mahu, dr. Alexandru Maizel, dr. Ana Marii Marinescu, dr. Adriana Eufrosina Moacă,

dr. Constantin-Didi Moșneguțu, dr. Liana-Ramona Moștenescu-Vasiliu, dr. Emil Năstase, dr. Doina Olteanu, dr. Mirela Liliana Oniceanu, conf. univ. dr. Carmen Pantiș, dr. Ladislau Pick, dr. Mihai Polinschi, dr. Daniela Popescu, dr. Andreia Radu, dr. Ion-Viorel Rădulescu, dr. Lucia Sereș, dr. Doina Sima, prof. univ. dr. Ileana Anca Sin, dr. Sinkó János, dr. Emilia Stamate, dr. Laurenția Ștefan, dr. Rodica Tănăsescu, dr. Emilia Tudoroiu,
dr. Voichița Varmaga, conf. univ. dr. Vlăduț-Doru Vasile, dr. Marcela-Georgeta Vidican, dr. Raluca-Oana Vodă, dr. Rareș Alexandru Zamfir.

Stimate colege,
Stimați colegi,

Este o mare plăcere și onoare să vă prezentăm acest **Ghid de Bune Practici în Protecția Datelor pentru Medicii din România**. Acest ghid a fost elaborat cu scopul de a oferi sprijin și orientare medicilor în general și echipei medicale în special, abordând o multitudine de aspecte legate de protecția datelor în contextul prelucrării informațiilor medicale sensibile și confidențiale.

Elaborarea acestui ghid a fost posibilă datorită contribuției conducerii Colegiului Medicilor din România, a membrilor Biroului Executiv, a membrilor colegiilor teritoriale și a partenerilor care ne-au oferit experiența și expertiza lor. Mulțumim tuturor celor care au contribuit cu spețe, întrebări și feedback pentru a asigura că acest ghid reflectă realitățile practice ale profesioniștilor din domeniul medical.

Ghidul a fost structurat în mai multe capitole, care detaliază atât bunele, cât și relele practici în protecția datelor medicale. Fiecare capitol oferă cazuri reale, amenzi aplicate și cazuistică relevantă din România și din Uniunea Europeană. În acest fel, sperăm să ajutăm medicii și echipa medicală să înțeleagă și să aplice în mod eficient principiile protecției datelor în activitatea lor de zi cu zi.

Adresabilitatea acestui ghid este în primul rând către medici, pentru a le oferi o resursă accesibilă și cuprinzătoare în materie de protecție a datelor. Avem în vedere să ne adresăm medicilor din România, indiferent de specializarea lor, respectiv de categoria de furnizor de servicii medicale unde își desfășoară activitatea și să îi ajutăm să navigheze cu încredere peisajul legislativ în materie de confidențialitate și protecție a datelor.

Pentru a face acest ghid cât mai accesibil și ușor de înțeles, vom pune la dispoziția publicului un website dedicat (www.gdpr.cmr.ro) care va include ghidul în format digital, consultări publice și materiale multimedia, precum filmulețe, tutoriale, podcasturi care rezumă anumite capitole sau studii de caz. În acest fel, dorim să asigurăm o abordare inovatoare și adaptată nevoilor medicilor și echipei medicale din era digitală.

Acest ghid reprezintă un efort important în promovarea unor bune practici în protecția datelor și în sprijinirea medicilor în îndeplinirea obligațiilor lor legale în acest domeniu. Ne mândrim cu realizarea acestui proiect și suntem încrezători că va servi drept o resursă valoroasă și utilă pentru medicii din România.

Cu speranța că acest ghid vă va oferi informațiile și îndrumarea necesară în protejarea datelor medicale și în respectarea drepturilor pacienților, vă dorim lectură plăcută și succes în aplicarea acestor principii în activitatea dumneavoastră profesională!

Așa cum ne aflăm într-o lume în continuă schimbare și evoluție, vom urmări să actualizăm și să adaptăm acest ghid pe măsură ce apar modificări legislative și tehnologice în domeniul protecției datelor. Prin aceasta, ne angajăm să sprijinim comunitatea medicală în a se menține la curent cu cele mai bune practici și cu cerințele legale în vigoare.

De asemenea, vă încurajăm să ne transmiteți orice feedback, sugestii sau întrebări pe care le aveți cu privire la conținutul acestui ghid la adresa de e-mail dpo@cmr.ro. Experiența și cunoștințele dumneavoastră practice vor contribui în mod semnificativ la îmbunătățirea și adaptarea acestui ghid pentru a răspunde cât mai eficient nevoilor comunității medicale.

Suntem recunoscători pentru încrederea pe care o acordați acestui ghid și pentru angajamentul dumneavoastră în protejarea datelor medicale și a drepturilor pacienților. Împreună, putem asigura un sistem de îngrijire a sănătății în care informațiile medicale sunt tratate cu respectul și protecția cuvenită.

Vă dorim succes în implementarea acestor bune practici și vă stăm la dispoziție pentru orice îndrumare și sprijin în acest demers. Colegiul Medicilor din România este alături de dumneavoastră în această călătorie spre o mai bună protecție a datelor și a vieții private a pacienților.

Cu deosebită considerație,

Responsabilul cu Protecția Datelor
Colegiul Medicilor din România

Despre protecția datelor cu caracter personal

În contextul în care societatea noastră devine din ce în ce mai conectată digital, protecția datelor personale și securitatea informațiilor au devenit aspecte cruciale, mai ales în domeniul sănătății. Drept urmare, acest ghid este conceput să ofere medicilor o perspectivă cuprinzătoare asupra importanței și implementării protecției datelor în practica medicală.

Evoluția Legislativă și Importanța Protecției Datelor în Sănătate:

În ultimii ani, țările europene au adoptat legi mai stricte în domeniul protecției datelor și securității cibernetice. Aceste schimbări legislative au avut un impact semnificativ asupra sistemelor de informații despre sănătate și a activităților de sănătate publică în general. Asemenea legi subliniază că dreptul la protecția datelor nu este absolut, ci trebuie echilibrat cu alte drepturi fundamentale și interese publice, cum ar fi dreptul la sănătate.

Evoluția legislației privind protecția datelor de la Directiva 95/46/CE la Regulamentul General privind Protecția Datelor (GDPR) marchează o tranziție semnificativă în abordarea dreptului la confidențialitate și protecția datelor personale în Uniunea Europeană. Directiva 95/46/CE, adoptată în 1995, a fost primul cadru legislativ major care a definit principiile fundamentale ale protecției datelor în Europa. Această directivă a stabilit reguli privind prelucrarea datelor personale și a acordat cetățenilor dreptul de a controla cum sunt utilizate informațiile lor personale. Cu toate acestea, întrucât era o directivă, implementarea sa varia de la un stat membru la altul, ceea ce a dus la un nivel de protecție inegal și adesea fragmentat.

R.G.P.D. (Regulamentul General privind Protecția Datelor), devenit aplicabil în mai 2018, a fost un pas major înainte, oferind un cadru unic și cuprinzător la nivelul întregii Uniuni Europene. R.G.P.D. a introdus noi drepturi pentru persoanele vizate, a impus adesea obligația numirii unui Responsabil cu Protecția Datelor și a stabilit reguli mai stricte pentru transferul de date în afara UE. De asemenea, R.G.P.D. a introdus obligația de a raporta încălcările de securitate ale datelor și a impus amenzi semnificative pentru nerespectarea prevederilor legale. Această evoluție reflectă o recunoaștere crescândă a importanței protecției datelor personale într-o lume tot mai digitalizată și interconectată.

Principii de Bază ale Protecției Datelor:

Protecția datelor se bazează pe principiile prevăzute în art. 5 din R.G.P.D. Între acestea se numără principii precum legalitatea, minimizarea datelor și limitarea scopului. Aceste principii asigură că datele sunt prelucrate doar într-un cadru de siguranță pentru persoanele vizate.

Definiții Fundamentale:

R.G.P.D. impune în „primele rânduri” câteva concepte cheie care sunt foarte importante de a fi reținute: date cu caracter personal, prelucrare de date, persoană vizată, operator de date, persoană împuternicită de operator, date sensibile.

- **Date cu Caracter Personal:** Acestea reprezintă orice informații legate de o persoană fizică identificată sau identificabilă. Exemplu: numele, adresa de email sau un număr de identificare.

- **Date Sensibile:** Acestea sunt categorii speciale de date personale care dezvăluie originea rasială sau etnică, opinii politice, convingeri religioase sau filozofice, apartenența sindicală, precum și prelucrarea datelor genetice, datelor biometrice în scopul identificării unice a unei persoane fizice, datelor privind sănătatea sau datelor privind viața sexuală sau orientarea sexuală a unei persoane. Un exemplu ar fi informațiile despre istoricul medical sau testele genetice ale unui pacient.

- **Prelucrare de Date:** Se referă la orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal. Exemple includ colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea.

- **Persoană Vizată:** Este persoana fizică la care se referă datele cu caracter personal. De exemplu, un pacient regăsit într-un registru medical este persoana vizată.

- **Operator de Date:** Entitatea (persoană fizică sau juridică, autoritate publică, agenție sau alt organism) care determină scopurile și mijloacele de prelucrare a datelor personale. Exemplu: un spital sau o clinică medicală privată;

- **Persoană Împuternicită de Operator:** Este o entitate sau chiar o persoană fizică (uneori) care prelucrează date cu caracter personal în numele operatorului de date. De exemplu, un laborator medical care efectuează teste de laborator pentru un spital.

Fiecare dintre aceste concepte joacă un rol esențial în cadrul R.G.P.D., subliniind importanța și complexitatea protecției datelor în contextul modern.

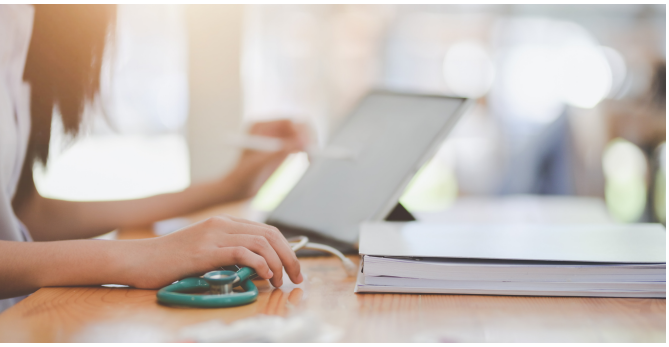
Implicații în Practica Medicală:

Protecția datelor este esențială în medicină, unde confidențialitatea și drepturile pacienților sunt de o importanță vitală. Legile actuale de protecție a datelor împuternicesc pacienții și persoanele vizate în general (ex. aparținători), astfel ca aceștia să-și exercite drepturile liber într-o lume dominată de tehnologie și prelucrarea masivă a datelor.

În câteva rânduri, protecția datelor cu caracter personal nu este o activitate unică, ci necesită o abordare sistematică și continuă. Aceasta implică responsabilitate instituțională, evaluare periodică a riscurilor și documentarea riguroasă a activităților de protecție a datelor. Este esențial să avem acest lucru în minte, pentru ca astfel să înțelegem că fără o conștientizare a fenomenului protecției datelor, a tuturor angajaților din domeniul medical, riscurile pentru pacienți rămân mari întotdeauna.

Pentru a trata aceste riscuri, dorim să menționăm că acest ghid are scopul de a facilita înțelegerea și aplicarea celor mai bune practici în protecția datelor, adaptate la contextul unic al practicii medicale, din viața de zi cu zi a medicului (nu a instituției spitalicești!).

Colegiul Medicilor din România, vede protecția datelor mai mult decât o cerință legală, pentru noi, aceasta reprezintă și un angajament față de etica profesională a medicului și reprezintă fundamentul încrederii pacienților în medicii noștri.



PARTEA I | CAPITOLUL 2

INTRODUCERE ÎN PROTECȚIA DATELOR ÎN SISTEMUL MEDICAL ROMÂNESC

GHID DEZVOLTAT DE

ÎN COLABORARE CU GDPRComplet.ro

Protecția datelor cu caracter personal în sistemul medical românesc pare a fi adesea doar un deziderat și nu o realitate de zi cu zi. Astfel, sarcina asumată prin acest ghid este una fără de măsură de mare, iar rezultatele acestei munci pot fi adesea contestate sau considerate ca fiind insuficiente. În acest sens, prezentul ghid ar trebui privit ca o invitație la a face primul pas înspre universul protecției datelor în domeniul medical.

Nu ne-am propus niciun moment ca acest ghid să aibă un caracter foarte științific, ori să fie cel puțin exhaustiv în abordare, ci să reprezinte un instrument practic pe care medicii îl pot folosi în activitatea lor de zi cu zi, fie că sunt angajați ai unei unități medicale, fie că sunt administratori ai unei clinici sau pur și simplu dețin un cabinet individual. Cu toate acestea, am considerat potrivit ca pentru acei medici care sunt parte a unor comisii de specialitate, a unor comisii disciplinare, a unor grupuri de lucru în diverse programe de sănătate publică sau strategii ori pur și simplu au și pregătire juridică și sunt interesați să aprofundeze subiectul să detaliem câteva aspecte în partea de final a ghidului.

Pentru început însă ne vom rezuma la simpla enumerare a aspectelor abordate în speranța sădirii interesului în fiecare dintre cititori.

Citind secțiunea dedicată cadrului juridic, vom putea concluziona următoarele:

- minimul de protecție a datelor este nivelul stabilit de R.G.P.D.
- introducerea unor măsuri mai drastice cu privire la protejarea datelor medicale nu este oprită, dimpotrivă, adesea este încurajată

În continuare, s-ar putea să avem următoarele întrebări la care cei interesați să găsească răspuns:

- pentru ce avem o asemenea legislație?
- este necesar să cunoaștem întreaga legislație specifică protecției datelor?
- care sunt consecințele nerespectării ei și cine răspunde?
- cum ar putea un medic, care nu cunoaște complet toate reglementările din domeniul protecției datelor, să le și respecte?

Aceste întrebări și altele similare vor fi abordate în acest ghid, pentru a vă ajuta să înțelegeți de ce avem o asemenea legislație și cum poate fi respectată chiar și de către cei care nu sunt complet familiarizați cu toate detaliile ei.

Pe parcursul întregului ghid veți identifica adesea spețe (cauze relevante) din jurisprudența curților de justiție naționale sau internaționale (cum ar fi decizii ale Curții Europene a Drepturilor Omului). Ținem să menționăm că aceste spețe sunt adăugate tocmai pentru a înțelege mai departe de litera legii, spiritul („bunului simț") în care aceasta a fost scrisă și mai ales să deprindem bunele practici care reies din aceste spețe. Pentru aceasta a fost scrisă secțiunea **„Locul dreptului la protecția datelor medicale în sistemul juridic"** și totodată pentru aceasta, la sfârșitul tuturor capitolelor sau secțiunilor, veți identifica anumite cauze relevante subiectului protecției datelor în domeniul medical.

Odată ce s-a înțeles și stabilit cadrul juridic, în firescul logicii, este deosebit de important să înțelegem principiile protecției datelor cu caracter personal. Cele câteva cuvinte cheie (legalitate, scop specific, minimizare, securitate, confidențialitate, responsabilitate) reprezintă fundația pe care se construiește acest ghid și legislația în ansamblul ei. Astfel, în secțiunea **Principiile protecției datelor** dorim să vă trezim interesul și să vă facem conștienți că activitatea medicală se bazează pe standarde juridice și etice încorporate prin intermediul unui mecanism exterior esenței activității medicale: protecția datelor cu caracter personal. Astfel, vom aprofunda înțelegerea principiilor care stau la baza protecției datelor cu caracter personal, așa cum sunt acestea stipulate în legislația de protecție a datelor. Pe scurt, în câteva cuvinte, am căutat să ilustrăm principiile prin secțiunea **Zece pași esențiali pentru conformitatea la R.G.P.D.**, **pentru că acești pași au la bază, în esență, principiile.**

În oglindă cu principiile, drepturile persoanei vizate (în general, ale pacientului) sunt de o importanță crucială. Într-o comparație stilistică, conceptul de „drepturi ale persoanei vizate" este în oglindă cu conceptul de „principii de prelucrare a datelor cu caracter personal".

Capitolul Drepturile persoanei vizate (ale pacientului, de regulă, dar nu numai!) vă oferă informațiile necesare pentru a înțelege cum puteți respecta și proteja drepturile pacienților în activitatea dumneavoastră zilnică. Aspectele teoretice însă sunt completate de orientările practice referitoare la exercitarea drepturilor, cum ar fi: **solicitări de a avea acces la date, solicitări de ștergere, de transfer sau cazuri de opoziție la diverse prelucrări de date.**

Aceste secțiuni dedicate urmăresc să ilustreze intersecția dintre etica medicală, aspectele juridice și considerentele privind viața privată și demnitatea umană. Vă invităm să reflectați asupra acestor aspecte în timp ce parcurgeți rândurile acestui ghid.

Toate aceste aspecte dezvoltate pe larg nu înlocuiesc consultanța de specialitate în domeniul juridic sau în domeniul protecției datelor pentru operatori (spitale, clinici, cabinete individuale ș.a.), însă nădăjduim ca prin această invitație să vă alăturați unui forum mai larg de discuții pe această tematică, menit să creeze o cultură a protecției datelor în sistemul medical românesc.

Suntem conștienți că acest lucru nu se va realiza peste noapte și nu poate fi impus, însă încurajăm fiecare organizație (unitate medicală sau furnizor de servicii medicale) să țină seama de recomandări, deoarece doar și în acest fel se poate crea un mediu mai sigur și în mod direct mai de încredere în medici în particular și în sistemul medical în general. Mai devreme sau mai târziu, fiecare dintre noi devine pacient și căutăm încredere și siguranță în sistemul medical pe care îl construim.

Puterea de a face diferența între construirea și menținerea unei bune reputații în sistemul medical românesc sau erodarea acesteia stă în mâinile noastre, ale medicilor, în activitatea noastră de zi cu zi.

Pentru aceasta sperăm să găsiți folositoare atât aspectele teoretice dezvoltate pe larg, dar și orientările practice pe care vă invităm să le parcurgeți în continuare!

2.1 CEI ZECE PAȘI ESENȚIALI PENTRU CONFORMAREA LA R.G.P.D.

Vă prezentăm în continuare zece pași esențiali pentru a respecta viața privată și protecția datelor personale ale pacienților noștri:

- **Fiți responsabil:** Înțelegeți și respectați toate obligațiile care vă revin în cadrul R.G.P.D. și asumați-vă responsabilitatea pentru protecția datelor pacienților. Totul pornește de la noi! În funcție de rolul pe care îl ocupați, verificați responsabilitățile specifice, citiți **Partea a IV-a „Relevanța normelor R.G.P.D. în funcție de rolurile ocupate de un medic”**.

- **Identificați scopul**: Colectați și prelucrați datele cu caracter personal doar în scopuri clare, legitime și specifice, în interesul pacientului. Pentru utilizarea datelor în scopuri secundare citiți **„Orientarea 3.13 privitoare la utilizarea datelor cu caracter personal în scopuri secundare decât cele în care au fost colectate inițial”.**

- **Obțineți consimțământul:** Asigurați-vă că pacientul înțelege și consimte în mod explicit prelucrarea datelor sale personale în scopul stabilit, atunci când aceasta se cere! Citiți pe larg **„Orientarea 3.16 privind obținerea și gestionarea consimțământului persoanei vizate”**.

- **Limitați colectarea:** Colectați doar datele cu caracter personal strict necesare scopului pentru care sunt necesare („Less is more!”).

- Asigurați-vă că **nu păstrați datele colectate mai mult decât este necesar**. Vom avea în minte mereu termenul prevăzut de lege sau un „termen rezonabil”.

- **Mențineți exactitatea:** Verificați și actualizați datele pacienților pentru a asigura acuratețea și actualitatea acestora.

- **Folosiți măsuri de protecție adecvate:** Implementați măsuri tehnice și organizatorice adecvate pentru a proteja datele pacienților de accesul neautorizat, pierdere sau distrugere.

- **Fiți transparent:** Informați pacientul în mod clar și accesibil despre modul în care sunt colectate, prelucrate și protejate datele sale personale.

- **Oferiți acces la date:** Asigurați-vă că pacientul are dreptul să-și verifice, să rectifice sau să șteargă datele personale pe care le dețineți.

- **Oferiți posibilitatea de a se adresa mai departe:** Informați pacientul despre dreptul său de a depune o plângere la ANSPDCP în cazul în care consideră că drepturile sale au fost încălcate.

Respectarea acestor pași simpli și clari vă va ajuta să protejați în mod eficient datele cu caracter personal ale pacienților și să vă conformați cu prevederile R.G.P.D. În continuare, vă invităm să consultați **orientările specifice** pe care le-am elaborat, pentru a înțelege pe larg responsabilitățile avute de către medici, în funcție de rolul ocupat. Pentru aceasta considerăm oportună identificarea rolurilor pe care le jucați în calitate de medic (Partea a IV-a „Relevanța normelor R.G.P.D. în funcție de rolurile ocupate de un medic”) și mai apoi parcurgerea orientărilor specifice, mai ales conform relevanței identificate de noi.

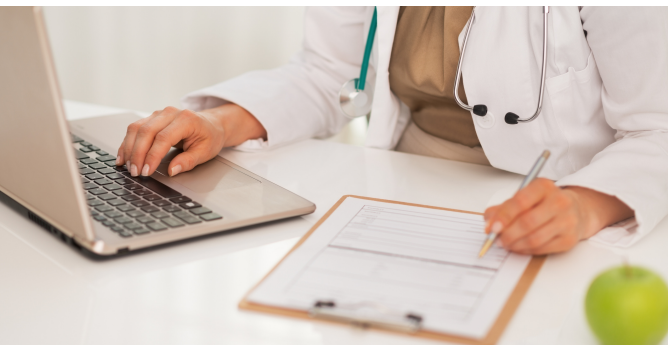
Pentru o aprofundare a studiului protecției datelor, a conceptelor, a felului în care diverse elemente legislative interacționează înspre protejarea datelor pacienților, vă rugăm să parcurgeți și Partea a III-a "Prelucrarea și protecția datelor în sănătate: De la cadrul legal la drepturile pacienților. Considerații pe larg".

Partea a IV-a - Resurse utile pentru medici (legislație, modele de documente, formulare) vă pune la dispoziție minimul de instrumente de care puteți avea nevoie pentru a respecta un nivel optim de viață privată a persoanelor cu care interacționați. În toate cazurile considerăm că este oportun să citiți ghidul în integralitatea sa întrucât în acest fel vă puteți face o imagine de ansamblu asupra aspectelor specifice pe care le implică această dinamică a respectării vieții private a persoanelor din jurul nostru.










PARTEA a II-a | CAPITOLUL 3

INTRODUCERE ÎN ORIENTĂRILE SPECIFICE PROTECȚIEI DATELOR

GHID DEZVOLTAT DE

ÎN COLABORARE CU GDPRComplet.ro

În această a doua parte a ghidului ne propunem să abordăm o serie de orientări specifice cu privire la protecția datelor în cadrul practicii medicale. Astfel, în următoarele pagini, vom discuta în detaliu fiecare orientare și vom prezenta recomandări practice pentru a vă asigura conformitatea cu R.G.P.D. și protejarea datelor personale ale pacienților în activitatea medicală.

Necesitatea și utilitatea acestei Părți a II-a a ghidului rezidă în faptul că, în contextul schimbărilor numeroase în ceea ce privește prelucrările de date, medicii se confruntă cu provocări și responsabilități semnificative în ceea ce privește gestionarea datelor cu caracter personal ale pacienților. Așadar, este esențial să se asigure o înțelegere clară și actualizată a obligațiilor pe care le au în acest sens, precum și a celor mai bune practici pe care le pot urma.

Pentru a răspunde acestor nevoi, Partea a II-a a ghidului a fost concepută astfel încât să ofere orientări practice, specifice și aplicabile în situații concrete, pentru a facilita conformitatea cu R.G.P.D. și a proteja confidențialitatea datelor pacienților. Această secțiune a ghidului este deosebit de utilă întrucât abordează aspecte diverse, dar cruciale, ale protecției datelor în activitatea medicală, precum gestionarea datelor, securitatea datelor în mediul digital, utilizarea dispozitivelor mobile și oferirea de servicii de telemedicină.

Prin includerea unor exemple relevante și cazuistică specifică, precum și a informațiilor despre amenzi aplicate, acest ghid oferă atât informații teoretice, cât și un context practic care să permită medicilor să înțeleagă și să aplice mai ușor principiile și regulile prezentate.

În plus, în multe dintre orientări veți găsi trimiteri către Partea a IV-a a ghidului, care include materiale practice, formulare și modele de documente, reprezintă o resursă suplimentară valoroasă, care îi ajută pe medici să-și îndeplinească obligațiile în materie de protecție a datelor, într-un mod eficient și coerent. Astfel, Partea a II-a a ghidului se dovedește a fi nu doar necesară, ci și extrem de utilă pentru profesioniștii din domeniul medical care doresc să acționeze în conformitate cu reglementările în vigoare și să-și protejeze pacienții și reputația profesională.

3.1 ORIENTĂRI PRIVIND ACORDURILE DE CONFIDENȚIALITATE ȘI CONTRACTELE DE SERVICII ÎNCHEIATE CU MEDICII ANGAJAȚI SAU COLABORATORI

- Enumerarea unor elemente cheie care trebuie incluse la nivelul contractelor prin care se prelucrează date cu caracter personal
- Prezentarea riscurilor neluării măsurilor organizatorice de actualizare a contractelor
- Prezentarea clauzelor contractuale model

În desfășurarea activității profesionale, medicii și personalul medical interacționează cu o varietate de parteneri cu care furnizorul de servicii medicale, adică operatorul (cabinetul medical, clinica, unitatea spitalicească, entitatea de îngrijiri medicale organizată sub orice formă) are încheiate sau va încheia contracte de furnizare de servicii.

În acest context, operatorul care va face prelucrări de date cu caracter personal necesare executării viitoarelor contracte de servicii este cel care **își alege parteneri prin care să desfășoare aceste activități** precum: *curierat, reparații laptopuri sau telefoane, mentenanță infrastructură informatică, mentenanță sistem de supraveghere video, contracte de colaborare cu alți medici, specialiști sau diverse laboratoare cărora li se trimit informații care pot cuprinde date cu caracter personal.*

În virtutea **principiului responsabilității operatorului** acesta trebuie să ia toate măsurile necesare pentru a se asigura că **atât personalul propriu cât și partenerul asigură un nivel înalt de securitate și confidențialitate a datelor!**

Clauze de asigurare a confidențialității și securității datelor

Pentru a se asigura de cele menționate anterior este recomandat ca operatorul să ia măsuri precum cele referitoare la:

- **Identificarea datelor cu caracter personal prelucrate de către angajat, respectiv de către partener**
  Exemplu: o firmă de curierat care a contractat serviciile unei clinici medicale sau ale unui laborator de recoltare a probelor biologice, în serviciul prestat, va stoca temporar buletinele de analiză transmise dintr-o locație în alta. Neasigurarea unui cadru de securitate și confidențialitate a acestui proces poate atrage sancțiuni clinicii. Există sancțiuni aplicate în România pentru lipsa selectării unui furnizor de servicii specializat care oferă un nivel ridicat de protecție în cadrul transferurilor pe care le efectuează. Această lipsă de responsabilitate a dus la următoarea situație: șoferul mașinii care transportă pachetul clinicii intuiește că în acesta pot fi și bani, deschide pachetul, ia banii, însă fără să vrea compromite probele biologice.

- **Identificarea scopurilor și naturii prelucrării**
  Exemplu: O firmă de dezvoltare soft oferă mentenanță unei aplicații informatice în care sunt introduse datele pacientului – scopul acestui acces este pentru a remedia eventualele probleme.

- **Identificarea temeiurilor legale, duratei prelucrării dar și măsurilor necesare pentru a proteja datele**
  Exemplu: Un medic colaborator va prelucra în baza contractului avut cu clinica medicală, datele pacienților. Acesta va avea acces la o multitudine de date medicale pe care le va introduce într-un sistem. Acestuia i se creează o adresă de email profesională – a clinicii – de pe care poartă conversația. La încetarea colaborării, întregul acces va fi retras. Pentru a prelucra datele, medicul se obligă contractual să nu divulge și să nu folosească toate aceste date în scopuri secundare.

- **Consecințele care pot apărea în cazul nerespectării obligațiilor contractuale asumate**
  Exemplu: Divulgarea datelor în cazul de mai sus, furtul bazei de date sau

folosirea în alte scopuri poate plasa medicul într-o zonă de nelegalitate și astfel să atragă asupra sa sancțiuni în cazul apariției unei investigații.

Pentru a ajuta medicii care administrează cabinete individuale medicale, ori clinici respectiv laboratoare medicale, vă punem la dispoziție:

- un model de clauze care ar trebui preluate în relație cu angajații (**Anexa nr.1 - Model de clauze care ar trebui preluate în relație cu angajații**)

- un model de acord de confidențialitate pe care să îl utilizați în relație cu colaboratorii persoane împuternicite, cu furnizorii de servicii sau cu cei care acționează în numele și pe seama operatorului (**Anexa nr.2 - Model de acord de confidențialitate pe care să îl utilizați în relație cu colaboratorii PÎ**).

Ce ar trebui să cunoașteți în calitate de administrator al unui S.R.L. respectiv al altei forme juridice de organizare a profesiei:

Înainte de a încheia un contract cu un furnizor de servicii extern (ex: servicii de arhivare, de distrugere a documentelor, de traduceri) sau un colaborator (ex: medic care prestează servicii în baza unui contract) trebuie să ne asigurăm că:

- Măsurile de confidențialitate și securitate a datelor luate de către furnizor sau de către medic sunt cel puțin la fel de ridicate ca cele luate de către cabinet / spital

La întocmirea contractului, în completarea aspectelor de mai sus, este bine să ținem cont de:

- Tipologia de acțiuni permise
- Procedurile specifice prin care se poate avea acces la date – spre exemplu să nu lucreze cu subcontractori decât cu acceptul scris al operatorului
- Să notifice operatorul în cazul în care anumite date au fost pierdute, furate, utilizate sau accesate în mod neautorizat
- Să raporteze în cel mai scurt timp orice încălcare la adresa confidențialității sau securității datelor
- Să returneze datele sau să le distrugă de îndată ce se încheie contractul (ex: orice fel de documente originale sau copii să fie predate operatorului, toate dispozitivele mobile să fie returnate ș.a.)

Cazuistică relevantă

O rea practică în acest context ar fi aceea în care un angajat al clinicii medicale (ex. un asistent medical) folosește accesul la datele cu caracter personal ale pacienților pentru a le vinde unui terț (ex. o companie de marketing farmaceutic). Această acțiune ar încălca normele de confidențialitate și securitate a datelor, precum și obligațiile contractuale asumate de angajat.

Medicover SRL – o persoană a trimis unui client un email care conținea actele adiționale ale contractelor de prestări servicii medicale care aparțineau altor clienți ai operatorului. Astfel au fost divulgate date precum: nume, prenume, CNP, adresă, semnătură. Amenda aplicată a fost de 1000 €.

(https://www.dataprotection.ro/?page=Comunicat_Presa_24_11_2022&lang=ro)

3.2 ORIENTĂRI PRIVIND ANGAJAMENTELE DE CONFIDENȚIALITATE ÎN RELAȚIILE DE MUNCĂ

- Enumerarea măsurilor care trebuie luate în raporturile de muncă de către un operator (o unitate medicală, o clinică, un spital ș.a.) pentru a respecta normele specifice protecției datelor
- Explicarea conținutului și importanței existenței acestor norme
- Exemple concrete și cazuistică relevantă

Fie că medicul este angajat al unei unități medicale (spital, clinică ș.a. numit generic operator de date), fie că ocupă o funcție de conducere în această unitate sau, mai mult, este administratorul ei, se impun a fi luate măsuri specifice protecției datelor în relațiile de muncă desfășurate în acea unitate.

Pentru aceasta, din momentul semnării contractului individual de muncă (C.I.M.), a fișei postului, a luării la cunoștință de Regulamentul Intern, angajatului - medic i se recunosc anumite drepturi și i se impun anumite obligații.

În rândurile care urmează ne propunem să atingem acest subiect: ce clauze relevante există sau pot fi adăugate la nivelul documentelor menționate mai sus pentru a fi în conformitate cu normele R.G.P.D. Această secțiune nu caută să acopere în mod exhaustiv toate măsurile care pot fi luate, ci doar să ușureze medicilor înțelegerea necesității existenței clauzelor de protecția datelor.

Astfel, în linii mari, indiferent de forma sub care apar, clauzele pot acoperi aspecte precum:

- **Obligația de confidențialitate:** Angajații (medici, asistenți medicali ș.a.) trebuie să păstreze confidențialitatea datelor cu caracter personal pe care le prelucrează și să nu le divulge terților fără autorizare expresă.

- **Obligația de a respecta bunele practici specifice protecției datelor cu caracter personal în relațiile de muncă:** Angajații trebuie să fie conștienți, respectiv să fie conștientizați, asupra bunelor practici de către unitatea medicală la care își desfășoară activitatea.

- **Obligația de a raporta încălcări ale securității datelor:** Angajații trebuie să raporteze orice încălcare a securității datelor la care au luat parte sau despre care au cunoștință.

Includerea acestor tipologii de clauze în documentele menționate (C.I.M., C.C.M., Fișa Postului, Regulament Intern) asigură în primul rând responsabilizarea angajaților, dar și evitarea sancțiunilor sau amenzilor care pot apărea atât pentru operator (unitate medicală) cât și pentru medic (atunci când acesta, în calitate de persoană fizică, devine operator de date).

Clauze relevante

Pentru a se asigura de cele de mai sus, este recomandat să fie incluse următoarele tipuri de clauze:

- **Regulament Intern (R.I.)**: obligația generală de respectare a principiilor R.G.P.D.; drepturile angajatului în calitate de persoană vizată; obligațiile acestuia; răspunderea sa.

- **Contract individual de muncă (C.I.M.)**: în principal ne rezumăm la drepturi și obligații specifice protecției datelor.

- **Fișa Postului**: aici putem identifica sau particulariza mai mult obligațiile care îi revin angajatului.

Toate acestea se regăsesc ca exemplu în **Anexa nr. 1** - *Model de clauze care ar trebui luate în relație cu angajații.*

Important de știut:

Sarcina probei în relațiile de muncă revine angajatorului - deși putem vedea în practică multe situații în care medicul, ca angajat al unei unități medicale, comite o faptă ce reprezintă un incident de securitate (ex. din eroare), operatorul, ca unitate medicală, este cel mai adesea sancționat pentru lipsa de: adoptare de politici și proceduri, instruire a persoanelor pentru a gestiona în mod corect datele cu caracter personal ș.a. În acest sens, fără a încuraja relele practici, medicul nu trebuie să fie speriat de apariția acestor clauze în contractele sale.

Exemplu: Un medic își folosește telefonul personal pentru a fotografia fișa medicală a unui pacient și apoi trimite fotografia unui coleg, încălcând astfel obligația de confidențialitate și securitate a datelor. În acest caz, prezența unei clauze în CIM și în Regulamentul intern care subliniază obligația de confidențialitate ar putea determina angajatorul să ia măsuri disciplinare împotriva medicului și să prevină astfel de situații în viitor. Lipsa dovezilor privind instruirea medicului de către unitatea medicală cu privire la acest aspect atrage responsabilitatea unității.

Procesul de conștientizare a fenomenului protecției datelor se realizează într-un mod mult mai eficient atunci când este asumat prin luarea la cunoștință a drepturilor și obligațiilor prin acest fel.

Exemplu: Un medic specialist primește o cerere de la un pacient să transmită fișa sa medicală unui alt medic, din afara unității medicale la care lucrează, pentru o a doua opinie. Medicul specialist nu verifică dacă are acordul pacientului pentru transferul datelor și nu urmărește procedura internă stabilită de către unitatea medicală pentru astfel de situații. Prin urmare, medicul nu respectă prevederile GDPR și ale legislației naționale privind protecția datelor.

Cazuistică relevantă

Un medic radiolog, în timpul pauzei de masă, lasă deschis pe ecranul laptopului o imagine radiologică a unui pacient, într-un spațiu accesibil altor angajați și vizitatori. Acest comportament expune datele cu caracter personal ale pacientului, încălcând normele de confidențialitate și securitate a datelor. Prin includerea unor clauze specifice în CIM, fișa postului și Regulamentul intern, angajații vor fi conștienți de responsabilitățile lor legate de protecția datelor și de consecințele nerespectării acestor prevederi.

Sentinta nr. 2280/2017 din 07-nov-2017 a Tribunalului Neamț: În acest caz, acțiunile asistentei medicale de a înregistra convorbiri între pacienți și medici și de a scoate în afara unității medicale acte medicale care conțin informații personale ale pacienților încalcă principiile de protecție a datelor cu caracter personal prevăzute în GDPR. Prin urmare, această speță este relevantă pentru GDPR, deoarece subliniază importanța respectării regulilor privind protecția datelor personale în contextul muncii și sancțiunile care pot fi aplicate în cazul nerespectării acestora.

3.3 ORIENTĂRI PRIVIND ACCESUL ȘI UTILIZAREA BAZELOR DE DATE

Prezentarea celor mai bune și a celor mai rele practici în accesarea și gestionarea bazelor de date electronice în unitățile medicale (clinici, spitale ș.a.), publice sau private, oferind exemple specifice și analizând o cauzuistică relevantă.

Tranziția de la înregistrarea datelor medicale pe hârtie la înregistrarea în sistemele electronice este o provocare continuă de aproape 20 de ani! În acest context al evoluției tehnologiei, a eficientizării muncii, dar și a apariției unui număr ridicat de provocări, atât pentru cabinetele medicale individuale, cât și pentru micile clinici ori unitățile spitalicești mai mari, protejarea confidențialității și securității datelor pacienților este deosebit de importantă!

Important de știut:

Etapa tranziției presupune mai multe aspecte pe care trebuie să le avem în vedere **atunci când facem parte din echipa de management sau suntem administratorul** unui S.R.L. sau a altei forme de exercitare a profesiei medicale. În continuare, prezentăm câteva practici cu acest rol:

Bune practici

Pași relevanți în procesul tranziției - Este important să putem face o tranziție de la înregistrările de pe hârtie la cele electronice (ex. introducerea unei noi platforme de înregistrare a pacienților și a unui nou mecanism de lucru), însă se recomandă a se ține cont de următoarele:

- **Revizuirea procedurilor de lucru și a politicilor de securitate pentru a se adapta la formatul electronic.** Astfel, managementul clinicii, spre exemplu, va decide împreună cu factorii relevanți metoda de lucru însă va trebui să comunice clar responsabilitățile angajaților sau colaboratorilor pe care îi are în subordine.

- **Actualizarea instruirii personalului în ceea ce privește confidențialitatea datelor și înregistrările electronice**. Provocările sunt foarte diferite, astfel anumite provocări sunt atunci când lucrăm cu documente fizice (ex. să le protejăm de a vărsa lichide peste acestea), unele diferite apar atunci când lucrăm cu înregistrări electronice (ex. verificarea cu antivirus a atașamentelor).

- **Păstrarea înregistrărilor medicale originale** (pe suport de hârtie sau electronic, după caz - spre exemplu o fișă a pacientului, o foaie de observație sau alt document în care sunt înregistrate aspecte referitoare la starea de sănătate a cuiva) până la tranziția completă în mediul online (pe suport electronic) și apoi distrugerea lor într-o modalitate sigură. Nu vom distruge documentele originale mai repede, de dragul de a „face spațiu” altor nevoi!

- **Salvarea copiilor scanate ale înregistrărilor pe hârtie în format „read-only ”**, procedură care asigură integritatea documentului și imposibilitatea de modificare și transmitere către terți neautorizați.

- **Păstrarea unei copii scanate sau a originalului (suport de hârtie)** în cazul utilizării tehnologiei OCR (Recunoaștere optică a caracterelor - utilizând tehnologia OCR, un document care este scanat sau o imagine care conține text poate fi transformată într-un fișier digitalizat, cum ar fi un document Word sau un fișier PDF care poate fi editat, permițând utilizatorului să interacționeze cu textul în multe moduri utile, cum ar fi căutarea unui anumit cuvânt sau expresie, editarea conținutului sau copierea și lipirea textului într-un nou document).

Stabilirea rolurilor - Accesul la înregistrările electronice trebuie să fie bazat pe roluri, protejând informațiile personale ale clienților prin aplicarea principiilor „nevoia de a ști” și „cel mai mic privilegiu”. Rolurile pot fi definite pentru toți utilizatorii, iar accesul la informații trebuie să fie acordat în funcție de necesitatea reală a acestora în îndeplinirea sarcinilor lor. Pe de altă parte, rolurile trebuie să fie reflectate de tipologia postului și de documentele juridice, precum contractul de muncă, actele adiționale la acesta și fișa postului.

- Nu este recoamandat ca un registrator medical sau o persoană cu atribuții de secretariat să aibă același nivel de acces la date medicale precum are medicul care supraveghează pacientul.

- Aici se poate stabili un mecanism de control acces prin restricționarea accesului la bazele de date electronice doar pentru personalul autorizat și instruit. **Exemplu:** Implementarea autentificării în doi pași și a permisiunilor bazate pe roluri pentru personalul medical și administrativ. Pe scurt, acest proces presupune:
    - **Utilizatorul își introduce numele de utilizator și parola**: Acesta este primul pas în procesul de autentificare. O căsuță de text arată unde utilizatorul își introduce numele de utilizator și parola.
    - **Serverul validează numele de utilizator și parola**: O săgeată duce de la căsuța de text către un simbol al unui server sau cloud, reprezentând serverul care verifică dacă numele de utilizator și parola sunt corecte.
    - **Serverul trimite un cod de verificare:** Dacă numele de utilizator și parola sunt corecte, o săgeată duce de la server către un telefon mobil, reprezentând serverul trimițând un cod de verificare prin SMS sau aplicație de autentificare la dispozitivul mobil al utilizatorului.
    - **Utilizatorul introduce codul de verificare**: O căsuță de text arată unde utilizatorul introduce codul de verificare primit.
    - **Serverul validează codul de verificare**: O altă săgeată duce de la căsuța de text către server, reprezentând serverul care verifică dacă codul de verificare introdus este corect.
    - **Autentificarea este reușită**: Dacă codul de verificare este corect, un semn de bifare sau un simbol similar indică faptul că autentificarea a fost reușită și utilizatorul are acum acces la contul sau serviciul protejat.

Stabilirea permisiunilor/atribuțiilor în funcție de pregătirea profesională și de implicarea în procesul de acordare a serviciilor medicale: strâns legat de roluri este stabilirea aspectelor permise pentru fiecare rol în parte, astfel anumite documente vor putea fi doar citite de personal, pe altele se va putea interveni prin scriere sau altele vor putea fi chiar și printate.

Măsuri de asigurare a securității și confidențialității - Medicii sunt responsabili pentru protecția datelor și accesul la date personale. Accesul bazat pe roluri trebuie să fie combinat cu alte măsuri de securitate, cum ar fi:

- deconectarea automată a utilizatorului din sistem după un interval stabilit de timp în care operatorul pe calculator / stația de lucru a devenit inactiv
- criptarea puternică
- gestionarea conturilor de utilizator
- declarații de confidențialitate și proceduri solide de backup și recuperare

!NB – La nivelul echipei manageriale din cadrul unui ambulator integrat / clinică privată / medic organizator al propriului cabinet de practică medicală, atunci când determinăm rolurile și permisiunile alocate este foarte util să ne întrebăm următoarele:

- Pot utilizatorii existenți să acceseze în prezent toate informațiile existente în server / platforma de lucru folosită?
- Pacientul poate să sufere vreo daună dacă utilizatorul are acces la informațiile sale medicale?
- Fiecare dintre aceste roluri alocate are cu adevărat nevoie de acces la toate câmpurile disponibile?
- Angajații și colaboratorii care activează în infrastructura noastră IT (în platformă) își pot îndeplini sarcinile de muncă (înscrise în fișa postului ori ca obligații contractuale asumate) dacă nu au acces la toate datele distribuite?
- Utilizatorul are nevoie de un acces regulat, zilnic, la informațiile medicale, sau are nevoie doar de acces ocazional?
- Există alte metode de acces mai facil cu riscuri mai mici?
- Care sunt domeniile funcționale posibile în care aceste informațiile medicale ar putea fi accesate (de exemplu, administrativ, clinic, financiar/facturare)?
- Care sunt toate permisiunile posibile care ar putea fi atribuite fiecărui rol (de exemplu, creare document, doar citire, actualizare, ștergere)?

Rele practici

Neglijarea confidențialității și securității - Lipsa măsurilor de securitate adecvate, precum protecția prin parolă, firewalls și actualizări de securitate, poate expune datele la riscuri majore. O rea practică este nerespectarea confidențialității și securității datelor pacienților, cum ar fi partajarea de informații personale ale pacientului fără consimțământul acestuia sau lăsarea deschisă a fișierelor electronice care conțin date sensibile.

- **Exemplu:** un angajat care lasă deschis un computer fără a se deloga (din platformă/aplicație, de pe contul de utilizator), permițând altor persoane să acceseze și să vizualizeze informațiile pacienților.

Acordarea de permisiuni excesive - O altă rea practică este acordarea de permisiuni excesive angajaților, ceea ce poate duce la accesul neautorizat la informații sensibile.

- **Exemplu**: un angajat cu rol de secretariat care are acces la toate înregistrările medicale ale pacienților, inclusiv la informațiile cu caracter confidențial, fără a avea nevoie reală de aceste informații în îndeplinirea atribuțiilor sale.

Atenție! Din perspectiva profesionistului, **„nevoia de a ști”** se poate transforma adesea în **„dorința de a ști”**, aspect care poate crea cel mai adesea probleme de securitate și confidențialitate a datelor.

Transmiterea necriptată a informațiilor - Trimiterea de informații sensibile, cum ar fi informațiile medicale ale pacienților, prin canale de comunicare nesecurizate.

- **Exemplu**: Trimiterea informațiilor pacienților prin e-mail fără criptare (fără a parola documentele) poate expune aceste informații foarte ușor.

Pentru a parola un fișier Word sau Excel, puteți utiliza următorii pași:

- Deschideți fișierul pe care doriți să îl parolați
- Faceți clic pe fila "Fișier" din partea de sus a ferestrei
- Selectați "Informații" din meniul vertical din stânga
- În partea dreaptă, faceți clic pe butonul "Protejează Document" sau "Protejează Caiet" (în Excel)
- Selectați "Criptează cu Parolă" din meniul derulant
- Introduceți parola pe care doriți să o utilizați și apoi apăsați "OK"
- Vi se va cere să reintroduceți parola pentru confirmare. Introduceți din nou parola și apăsați "OK"

Salvați documentul pentru a vă asigura că modificările sunt păstrate.

- **Gestionarea inadecvată a backup-urilor și recuperării datelor -** Acest lucru poate include lipsa unui sistem automat de backup, neprotejarea corespunzătoare a backup-urilor sau incapacitatea de a recupera rapid datele în caz de pierdere sau corupere a acestora.
  - **Exemplu:** o clinică unde nu se realizează backup-uri zilnice ale datelor electronice este expusă riscului de pierdere irecuperabilă a informațiilor medicale ale pacienților în cazul unei erori sau al unui atac cibernetic.

Cazuistică relevantă

Într-o clinică medicală dintr-un mic orășel de provincie, observând practicile concurenței nou apărute, conducerea a decis să treacă și ei la înregistrările electronice, dar fără să acorde suficientă atenție securității și confidențialității datelor. În loc să actualizeze procedurile de lucru și să instruiască angajații în utilizarea corectă a sistemului electronic, au trecut direct la implementarea noului sistem, fără a se pregăti corespunzător.

Rezultatul: angajații nu au știut cum să protejeze corect informațiile pacienților în mediul digital. Un registrator medical, care nu a primit instruire corespunzătoare, a trimis un e-mail necriptat unui coleg, cu informații sensibile despre un pacient, încălcând astfel confidențialitatea acestuia.

Mai mult, clinica nu a stabilit roluri și permisiuni adecvate pentru angajați, astfel că toți aveau acces la informațiile pacienților, indiferent de responsabilitățile lor. Un angajat al departamentului de facturare, de exemplu, putea vedea detaliile medicale intime ale pacienților, deși nu avea nevoie de aceste informații pentru a-și îndeplini atribuțiile.
În cele din urmă, lipsa de măsuri de securitate adecvate a dus la o încălcare a securității datelor, iar informațiile confidențiale ale pacienților au fost expuse. Această rea practică a atras atenția autorității de supraveghere, care a sancționat clinica și a afectat reputația ei în comunitate.

Autoritatea națională de supraveghere a investigat posibile încălcări ale legislației privind protecția datelor personale cauzate de postarea unor anunțuri de achiziții publice pe site-ul www.e-licitatie.ro de către o unitate spitalicească. Anunțurile conțineau date personale ale pacienților minori, precum nume, prenume și informații despre starea de sănătate (analize medicale).

Investigația a relevat că nu a existat un temei legal pentru diseminarea datelor personale ale minorilor și că unitatea spitalicească nu a implementat măsuri tehnice și organizatorice adecvate pentru a asigura un nivel de securitate corespunzător. Drept urmare, a avut loc divulgarea neautorizată și accesul neautorizat la datele personale ale pacienților minori pe site-ul menționat.

Unitatea spitalicească a primit un avertisment, deoarece nu a implementat măsurile de securitate necesare care au condus la divulgarea neautorizată a datelor personale ale pacienților minori prin postarea anunțurilor de achiziții publice în Sistemul Electronic de Achiziții Publice (SEAP).

Sursa: Raportul de activitate al A.N.S.P.D.C.P. pentru anul 2020.
Link: *https://www.dataprotection.ro/?page=Rapoarte%20anuale&lang=ro*

Cazuistică din U.E:

Centro Hospitalar Barreiro Montijo a fost amendat cu 400.000 de euro pentru încălcarea Regulamentului General privind Protecția Datelor (GDPR). Autoritatea de supraveghere din Portugalia, Comissão Nacional de Protecção de Dados (CNPD), a identificat trei încălcări ale GDPR:

- **Încălcarea principiului de minimizare** prin permiterea accesului necontrolat la un număr excesiv de utilizatori, amendată cu 150.000 de euro. În mod concret: orice doctor putea accesa datele pacienților oricărui alt coleg asistent medical, indiferent de specializarea acestuia.
- **Încălcarea integrității și confidențialității** prin neaplicarea măsurilor tehnice și organizatorice pentru a preveni accesul neautorizat la datele personale, amendată cu 150.000 de euro.
- **Incapacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și reziliența continuă a sistemelor și serviciilor de tratament**, amendată cu 100.000 de euro.

CNPD a acționat în urma unui articol publicat într-un ziar, nu a unei plângeri. Printre faptele considerate dovedite de CNPD se numără lipsa documentelor care să stabilească corespondența între competențele funcționale ale utilizatorilor și profilurile de acces la informații (în mod concret existau 985 utilizatori ca „doctor” deși în spital erau angajați doar 296), precum și existența unor profiluri inutile pentru medici care nu mai lucrează în spital. CNPD a ținut cont de aceste aspecte și de faptul că datele implicate erau categorii speciale de date în determinarea sumei amenzii. Sursa: *https://iapp.org/news/a/first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations/*

3.4 ORIENTĂRI PRIVIND ASIGURAREA EXACTITĂȚII ȘI INTEGRITĂȚII DATELOR MEDICALE ÎNREGISTRATE

- Sublinierea importanței menținerii exactității și integrității datelor medicale înregistrate de medici;
- Furnizarea unor recomandări cu privire la verificarea și actualizarea datelor medicale.

Menținerea exactității și integrității datelor medicale înregistrate de medici este **esențială** pentru asigurarea calității îngrijirii pacienților și respectarea prevederilor legale, cum ar fi Regulamentul General privind Protecția Datelor (GDPR). Pentru a atinge aceste obiective, medicii și personalul medical trebuie să adopte practici adecvate în ceea ce privește **verificarea și actualizarea datelor pacienților.**

Aspectele principale de care trebuie ținut cont sunt următoarele: implementarea unor proceduri de verificare și actualizare regulată a datelor medicale, precum și promovarea unei culturi organizaționale care să pună accent pe importanța exactității datelor înregistrate.

Important de știut!

Documentarea corectă și completă a datelor medicale este esențială pentru a putea oferi o îngrijire adecvată pacienților și pentru a evita erorile medicale.

Exemplu: Un pacient este rugat să completeze formularul de înscriere sau fișa de înregistrare în sistem. Acesta nu respectă procedura internă și menționea că ar trebui să scrie cu majuscule în acest document, astfel că scrie emailul cu litere mici. Datorită unei erori, medicul citește litera „a” ca fiind litera „o” și astfel transmite buletine de analize medicale către o altă adresă de email decât cea a pacientului care a completat fișa. Pacientul reclamă o divulgare neautorizată de date.

- Recomandarea noastră se adresează întregului personal medical care lucrează cu documente medicale și cu datele pacienților. Este esențială o atenție sporită și o revizuire riguroasă a procesului de înregistrare a datelor furnizate de pacienți, pentru a ne asigura că informațiile sunt corecte, complete și actualizate. În special, dacă intenționați să trimiteți documente medicale în format electronic, este crucial să verificați adresa de e-mail a pacientului. O adresă de e-mail incorectă sau neactualizată poate duce la probleme serioase, inclusiv încălcări ale confidențialității și probleme de comunicare.

Revizuirea periodică a datelor înregistrate în dosarele medicale ale pacienților contribuie la identificarea și corectarea posibilelor erori sau omisiuni. Atunci când anumite date nu se mai justifică a fi păstrate sau trebuie înlocuite, ar trebui să facem acest lucru.

Exemplu: păstrarea unei copii a cărții de identitate s-ar putea să fie necesară în anumite situații. Persoanele însă își schimbă uneori numele, prenumele sau cărțile de identitate expiră după o anumită perioadă și trebuie înlocuite, astfel că seria și numărul acesteia se schimbă. Unitatea medicală sau medicul ar trebui să pună în vedere pacientului necesitatea prezentării noii cărți de identitate pentru a asigura principiul exactității datelor.

- Fie că pacientul se prezintă pentru o consultație de rutină sau este internat în spital este esențial să ne asigurăm că datele sale de identitate sunt actualizate și corecte. Această verificare nu trebuie să se limiteze doar la numele și prenumele pacientului, ci trebuie să includă și validarea perioadei de valabilitate a actului de identitate. Acest lucru nu doar că ajută la menținerea acurateții înregistrărilor noastre, dar și facilitează o comunicare eficientă cu pacientul și poate preveni potențialele încălcări ale securității sau ale confidențialității. În plus, acest proces este benefic atât pentru unitatea medicală, cât și pentru pacient. Pentru unitatea medicală, asigură conformitatea cu reglementările privind protecția datelor și gestionarea eficientă a înregistrărilor pacientului. Pentru pacient, acesta îl conștientizează cu privire la importanța menținerii datelor de identitate actualizate și exacte.

Crearea și menținerea unor sisteme de raportare și monitorizare a erorilor din dosarele medicale poate ajuta la îmbunătățirea proceselor de gestionare a informațiilor și la prevenirea erorilor în viitor.

Exemplu: se notează într-un document centralizator situațiile problematice întâlnite pe parcursul unui an și se discută cu personalul relevant care sunt cele mai bune practici recomandate (Atașat găsiți un model - **Anexa 3** *Tabel centralizator urmărire monitorizare*).

Stabilirea și respectarea unui program securizat de acces la dosarele electronice de sănătate ale pacienților, evitându-se orice riscuri la adresa confidențialității modalităților de acces în sistem.

Exemplu: mulți pacienți au tendința nesănătoasă de a nu schimba parola inițială a cardului de sănătate, care cuprinde anul nașterii sau ultimele patru cifre ale CNP iar, ulterior, de a o divulga fără restricții. Pe cât posibil trebuie instruit și pacientul la momentul contextual potrivit că procedura de confidențialitate menține un echilibru adecvat în relația dintre pacient și medic.

- Asemenea unui card bancar, cardul de asigurat trebuie tratat cu maximă seriozitate și responsabilitate. Este esențial ca pacienții să înțeleagă importanța cardului de asigurat și să îl protejeze în mod adecvat. Acesta include păstrarea în siguranță a cardului și nu divulgarea informațiilor de pe acesta, cum ar fi numărul de asigurat, la fel ca și cum ar fi un PIN al unui card bancar. Astfel, deși greu de implementat în multe cazuri, ideal ar fi ca pacientul să introducă PIN-ul cardului pe calculatorul pe care operează medicul.

Bune practici pentru asigurarea exactității datelor medicale înregistrate de medici:

Verificarea și actualizarea regulată a datelor pacienților - Asigurați-vă că informațiile personale și medicale ale pacienților sunt corecte și actualizate, solicitându-le să confirme aceste informații în timpul fiecărei vizite.

Implementarea unui sistem electronic de înregistrare a datelor - Un sistem electronic de înregistrare a datelor medicale poate ajuta la reducerea erorilor și la facilitarea accesului la informații pentru toți membrii echipei medicale.

Pseudonimizarea sau anonimizarea datelor atunci când este posibil - Acest lucru poate ajuta la protejarea confidențialității pacienților în cazul în care datele sunt folosite în scopuri de cercetare sau statistice.

- **Educația și formarea personalului -** Asigurați-vă că personalul medical este instruit în mod corespunzător cu privire la importanța exactității datelor și la modul în care pot fi prevenite erorile.

- **Crearea și aplicarea unor politici și proceduri clare privind gestionarea datelor -** Acest lucru poate ajuta la stabilirea unor standarde clare și la promovarea unei culturi organizaționale care să pună accent pe exactitatea datelor.

Rele practici în asigurarea exactității datelor medicale înregistrate de medici:

- **Neglijarea verificării și actualizării datelor pacienților -** A nu solicita pacienților să confirme informațiile personale și medicale în timpul fiecărei vizite poate duce la erori și la divulgări neautorizate a datelor.

- **Lipsa de instruire a personalului -** Personalul medical care nu este instruit în mod corespunzător cu privire la importanța exactității datelor și la modul în care pot fi prevenite erorile este mai predispus să comită greșeli.

- **Ignorarea feedback-ului pacienților -** Dacă nu luați în considerare sugestiile sau reclamațiile pacienților cu privire la erorile în datele lor medicale, aceasta poate duce la deteriorarea relației dintre medic și pacient, sesizări, plângeri sau reclamații.

Cazuistică relevantă

Folosirea unui sistem ineficient de raportare și monitorizare a erorilor: Lipsa unui sistem eficient de raportare și monitorizare a erorilor din dosarele medicale, precum și a unui tabel de evidență pentru a analiza și corecta erorile, poate duce la repetarea acestor greșeli și la compromiterea calității îngrijirii pacienților.

O clinică nu folosește un tabel de evidență a erorilor pentru a monitoriza și raporta problemele legate de dosarele medicale. Personalul medical nu discută și nu analizează erorile întâlnite pe parcursul anului, ceea ce duce la persistența acestora și la neidentificarea unor posibile soluții pentru îmbunătățirea gestionării informațiilor. Această abordare lipsită de transparență și comunicare poate conduce în final la erori medicale și la divulgarea neautorizată a datelor pacienților.

Cazuistică din activitatea Autorității de Supraveghere:

Conform Raportului de Activitate al A.N.S.P.D.C.P. pentru anul 2021, un furnizor de servicii medicale a notificat Autoritatea Națională de Supraveghere cu privire la trei incidente de încălcare a securității datelor cu caracter personal. Acestea includ:

- În primul caz, un angajat al furnizorului de servicii medicale a transmis răspunsul către o persoană vizată/client la o adresă de e-mail greșită, care aparținea altei persoane. Acest lucru s-a datorat înregistrării de către un angajat al unității medicale, a unei adrese scrise olograf prin care persoana vizată adresa o reclamație. Unitatea medicală a dorit să transmită e-mailul de răspuns, însă a fost trimis eronat către o altă persoană vizată. Reclamantul a acuzat faptul că datele sale i-au fost dezvăluite unei terțe persoane.
- În al doilea caz, un angajat a transmis prin e-mail un contract de prestări servicii medicale către o altă persoană decât titularul de contract, dintr-o eroare umană. Contractul a fost transmis în mod securizat, folosind criptarea cu parolă, însă această situație a generat riscul de expunere a datelor personale ale pacientului.
- În al treilea caz, un plic conținând contractul unui viitor client al clinicii a fost trimis prin curier, însă în mod eronat, a fost inclus în același plic un alt contract aparținând unui alt client. Clientul care a primit contractul greșit a sesizat clinica și a predat contractul, dar acest incident a implicat o încălcare a confidențialității datelor cu caracter personal ale pacienților.

Sursa: *https://www.dataprotection.ro/?page=Rapoarte%20anuale&lang=ro*

3.5 ORIENTĂRI PRIVIND POSIBILITATEA DE FOTOGRAFIERE, REALIZAREA DE CAPTURI VIDEO ȘI ALTE IMAGINI FOLOSITE ÎN SERVICIUL MEDICAL

- Descrierea celor mai bune practici pentru protejarea datelor cu caracter personal atunci când se utilizează fotografii, imagini video, înregistrări vocale, vizuale, etc.

- Identificarea pașilor necesari de făcut înainte, în timpul și după fotografierea sau înregistrarea unei persoane

Înainte de a fotografia sau înregistra audio/video pacienții, medicii ar trebui:

- Să identifice în mod exact scopul pentru care dorește să facă acest lucru

- Să identifice temeiul legal aplicabil (**obligație legală, interes legitim, consimțământ**)
  - **Exemplul 1**: scopuri de marketing, promovare, publicitate – avem nevoie de consimțământ specific R.G.P.D.
  - **Exemplul 2**: cazul studiilor clinice, situație în care se vor anonimiza toate elementele care pot duce la identificarea persoanei fizice și în absența cărora studiile nu sunt afectate

Să aibă în vedere următoarele atunci când este vorba de **consimțământ**:

- deși consimțământul verbal este suficient, cele mai bune practici presupun faptul că pacientului i se pune la dispoziție un formular de consimțământ scris care să cuprindă informații relevante (inclusiv scopurile colectării, utilizării și divulgării, temeiul legal etc).
- model de consimțământ puteți găsi aici: **Anexa 4 Consimțământ specific R.G.P.D.**

Să obțină consimțământul de la:

- un părinte sau un tutore, în cazul în care pacientul este un copil care nu este capabil să își exercite drepturile legale
- un reprezentant personal în cazul în care un pacient este considerat incapabil juridic sau faptic

Să se asigure că persoana înțelege:

- scopul pentru care este realizată fotografia sau înregistrarea și modul în care va fi utilizată
- cui i se va permite accesul la aceasta
- cât timp va fi păstrată și cum va fi stocată, respectiv protejată
- că în lipsa consimțământului calitatea îngrijirii medicale va fi aceeași
- că acest consimțământ poate fi retras oricând

După fotografierea sau înregistrarea audio/video, cele mai bune practici prevăd că medicii ar trebui:

Să se asigure că toate fotografiile, înregistrările, imaginile sunt anonimizate sau pseudonimizate, după caz, prin ștergerea numelui pacientului

Să asigure un nivel de securitate ridicat pentru acestea prin stocarea lor în medii sigure (ex. pe un cloud cu acces limitat sau pe un hard disk critptat)

În cazul în care fotografiile, înregistrările, imaginile trebuie arătate unor terțe părți:

Informarea persoanei despre transferul / comunicarea datelor

Asigurarea unui cadru formal de securitate și confidențialitate a datelor

- Nu este o bună practică comunicarea unor rezultate de analize medicale prin Whatsapp către alți medici din alte unități medicale. Aceste practici sunt des întâlnite!

Ca regulă generală este bine de reținut faptul că:

Nu ar trebui să se facă nicio fotografie sau înregistrare contrar dorinței persoanei, atunci când vorbim de desfășurarea actului medical!

Totuși, în circumstanțe excepționale, **fotografierea sau înregistrarea poate fi realizată fără consimțământul pacientului:**

- **Exemplu**: pacientul este în imposibilitate de a-și da consimțământul sau nu poate face acest lucru în timp util sau devine lipsit de discernământ și cu toate acestea prelucrarea unor astfel de date (realizarea de fotografii) este în mod vădit realizată în interesul acestuia pentru a putea documenta tratamentul sau chiar pentru a salva interesele vitale ale acestuia.

Cazuistică relevantă

Un medic de familie deține un blog în care scrie despre diverse cazuri medicale interesante pe care le-a întâlnit în timpul carierei sale. Într-o postare recentă, medicul descrie un caz complex de diagnosticare a unei boli rare și, pentru a ilustra cât mai bine situația, decide să includă în articol fotografii cu rezultatele testelor medicale ale pacientului și imagini ale simptomelor specifice.

Cu toate că medicul a decis să nu menționeze numele pacientului în articol, a uitat să anonimizeze complet rezultatele testelor medicale și unele date personale ale pacientului, cum ar fi inițialele și vârsta, rămân vizibile. Mai mult, medicul nu a obținut consimțământul informat al pacientului înainte de a publica aceste informații pe blog.

Publicarea acestor date personale, fără consimțământul pacientului și fără anonimizarea corespunzătoare, reprezintă o încălcare a principiilor de confidențialitate și protecție a datelor cu caracter personal. Astfel, medicul ar putea fi supus unei amenzi din partea autorității de supraveghere pentru încălcarea prevederilor privind protecția datelor.

!NB - Este esențial ca, în procesul de comunicare a informațiilor medicale, să se evite divulgarea oricăror detalii care ar putea permite identificarea pacientului. Acest lucru include, dar nu se limitează la inițialele pacientului, sexul, vârsta sau orice alte caracteristici demografice sau de sănătate specifice care ar putea facilita identificarea.

Recomandăm utilizarea unor descriptori generali care să permită înțelegerea contextului cazului fără a dezvălui detalii personale. De exemplu, în loc să specificați **"Pacientul M.F., de sex feminin, în vârstă de 55 de ani..."**, ați putea spune **"Un pacient s-a prezentat cu..."**

Mai mult, în cazul în care se dorește folosirea de fotografii sau alte imagini în aceste contexte, este esențial să se obțină consimțământul explicit, informat și liber al pacientului, iar imaginile trebuie să fie anonimizate corespunzător.

Respectarea acestor practici nu numai că asigură conformitatea cu legile și reglementările privind protecția datelor, dar contribuie și la menținerea încrederii pacientului în sistemul de îngrijire a sănătății. Prin urmare, recomandăm adoptarea acestor practici ca standard în prezentarea cazurilor clinice sau științifice.

Cazuistică din activitatea Autorității de Supraveghere:

Autoritatea italiană pentru protecția datelor (Garante) a aplicat unui medic o amendă de 5.000 de euro. Operatorul a prezentat diapozitive ale unui caz clinic la un congres, care au fost ulterior publicate pe site-ul Società triveneta di chirurgia. Slide-urile conțineau date personale ale unui pacient, cum ar fi inițialele pacientului, vârsta, sexul, istoricul medical detaliat al pacientului, detalii ale internărilor din 1980 până în 2016 și procedurile chirurgicale efectuate în perioada respectivă, indicând data internării și data efectuării operațiilor, secția de chirurgie care a realizat procedurile, zilele petrecute în spital, numeroase imagini de diagnostic și 22 de fotografii care arată pacientul în timpul intervențiilor chirurgicale.

Persoana vizată (pacientul) nu și-a dat consimțământul pentru o astfel de prelucrare a datelor sale personale.

Sursa: *Ordinanza ingiunzione - 15 aprile 2021 - Garante Privacy*

3.6 ORIENTĂRI PRIVIND UTILIZAREA DISPOZITIVELOR MOBILE

- Sintetizarea riscurilor utilizării dispozitivelor mobile pentru furnizarea de servicii de asistență medicală
- Identificarea celor mai bune practici pentru utilizarea dispozitivelor mobile

Care sunt riscurile?

Dispozitivele mobile, cum ar fi telefoanele inteligente și tabletele, oferă un mod convenabil și eficient de a comunica cu pacienții și cu alți furnizori de servicii medicale de la distanță.

Cu toate acestea, utilizarea acestor dispozitive în cadrul unităților medicale prezintă riscuri pentru confidențialitate și securitatea informațiilor personale, cum ar fi pierderea sau furtul dispozitivului, infestarea cu programe rău intenționate care pot urmări sau spiona dispozitivul și interceptarea sau monitorizarea informațiilor personale de către părți neautorizate.

De asemenea, orice dispozitiv wireless, inclusiv un dispozitiv mobil, care este conectat la o rețea (de exemplu, Wi-Fi, Bluetooth, 3-4-5G și comunicarea în câmp apropiat) poate servi drept intrare pentru atacuri cibernetice, dacă nu este configurat cu controale de securitate adecvate.

Noile tehnologii trebuie receptate prin prisma RGPD, stabilindu-se în primul rând dacă aceastea prelucrează date medicale. Conceptul de **„prelucrare de date medicale”** este unul specific, combinând abordarea tehnică cu cea medicală.

Ca urmare, este util să cunoaștem că în toate următoarele trei scenarii, fluxul de date este calificat drept **„prelucrare de date personale cu caracter medical”**:

- datele prelucrate prin dispozitiv sunt în mod evident date personale cu caracter medical (ex. fotografia unui foi de observație)

- datele brute ale senzorilor, prelucrate prin aplicație sau dispozitiv, pot fi utilizate independent sau în combinație cu alte date, pentru a trage concluzii cu privire la starea reală a unui individ sau la riscurile pentru sănătate (ex. utilizarea unui dispozitiv de măsurare a tensiunii)

- pe baza datelor colectate prin aplicație sau dispozitiv se trag concluzii cu privire la starea de sănătate sau la riscurile pentru sănătatea unui anumit individ, indiferent de corectitudinea acestor concluzii (ex. în cazul unora dintre aplicațiile MyHealth).

Situații cu risc:

- **Date obținute prin acces neautorizat:** un hacker poate accesa datele cu caracter personal ale pacienților prin intermediul unui virus informatic sau unei vulnerabilități a sistemului de securitate al telefonului mobil al medicului.

- **Date pierdute:** datele cu caracter personal ale pacienților pot fi pierdute dacă telefonul mobil al medicului este furat sau distrus.

- **Încălcarea securității:** datele cu caracter personal ale pacienților pot fi compromise dacă telefonul mobil al medicului nu este protejat cu parole și criptare.

- **Crearea de duplicate:** datele cu caracter personal ale pacienților pot fi dublate prin intermediul unei conexiuni necesare sau prin copierea datelor pe alte dispozitive.

Cele mai bune practici

Unitățile medicale prin personalul acestora, pentru a respecta normele privind protecția datelor cu caracter personal trebuie să ia **măsuri tehnice și organizatorice** adecvate înainte de a utiliza dispozitivele mobile în practica lor. Această obligație se extinde la întreg personalul dar și la terții care au acces la date cu caracter personal care acționează sub îndrumarea operatorului de date (a unității medicale).

Este recomandat ca pentru activitățile profesionale să se aloce un **dispozitiv mobil distinct și exclusiv** dedicat acestui tip de activități. Unitățile mici, cum ar fi unele cabinete medicale individuale, pot apela la un specialist în protecția datelor în vederea realizării unui audit specific protecției datelor, în urma căruia i se vor indica măsurile de luat pentru ca activitatea sa să se realizeze în conformitate cu cerințele Regulamentului General privind Protecția Datelor.

În același timp, **preluarea unor reguli simple** este la îndemâna oricărui medic și au eficiența cea mai mare (exemplu: *interzicerea fotografierii sau a înregistrărilor audio-video în interiorul incintei, de către terți; utilizarea unui singur dispozitiv mobil electronic în scopuri profesionale etc*.).

!NB - Una dintre practicile existente în România la acest moment este următoarea: medicii nu dispun de telefoane sau cartele de telefon de serviciu atunci când își desfășoară activitatea în cadrul unui operator de date (spital public, spital privat), astfel încât toate comunicările în interes de serviciu sunt realizate prin propriul dispozitiv mobil. Aceste comunicări se realizează atât între colegii de muncă, cu superiorii sau cu echipa medicală, dar se întâmplă să existe astfel de comunicări și în relație directă cu pacienții.

Acest aspect creează adesea un nivel de disconfort ridicat pentru viața privată a medicilor, dar și riscuri ridicate pentru datele cu caracter personal ale pacienților sau ale colegilor de muncă.

În acest sens, se recomandă achiziționarea de telefoane mobile de serviciu sau cel puțin de cartele de telefon cu numere de serviciu, iar la debutul colaborării să fie puse la dispoziția medicilor. Atunci când resursele financiare nu permit astfel de cheltuieli, se pot alege și alte variante precum: achiziționarea cel puțin pe secție a unui telefon cu cartelă de serviciu sau la nivelul unei alte structuri, astfel încât relațiile de muncă să se poată desfășura în condiții de normalitate și eficiență!

Atunci când vă desfășurați activitatea folosindu-vă de un dispozitiv mobil, vă rugăm să aveți în vedere următoarele:

- **Asigurați-vă** că:
    - dispozitivele dispun de un sistem de criptare puternic, actualizat și la standarde industriale pentru transmiterea informațiilor personale, pentru a minimiza riscul de interceptare neautorizat
        - **Exemplu**: putem face actualizările periodice recomandate de soft și putem stabili o parolă complexă
    - orice sistem la care este conectat dispozitivul oferă o securitate adecvată de la un capăt la altul
        - **Exemplu**: ne ferim de rețelele wifi publice
    - funcțiile de comandă vocală sunt dezactivate în cazul în care nu sunt necesare, deoarece această funcție permite ca dispozitivul să fie mereu în ascultare!
    - ecranul este setat să se blocheze automat după o perioadă scurtă de inactivitate.

- **Întotdeauna**:
    - utilizați aplicații care provin din magazinele oficiale de aplicații și care utilizează o criptare puternică, actualizată și conformă cu standardele din domeniu
    - mențineți software-ul la zi

- **Raportați imediat pierderea sau furtul** unui dispozitiv și luați în considerare utilizarea programelor care vă ajută să vă localizați telefonul
        - **Exemplu**: dacă telefonul este de serviciu și conține date cu caracter personal pe acesta, anunțați superiorul ierarhic
        - Exemple de servicii pentru localizarea telefoanelor: "Find My iPhone" (iOS), "Find My Device" (Android) și "Windows Device Recovery Tool" (Windows)

- Atunci când returnați (pentru reparații) sau aruncați un telefon sau alt dispozitiv, asigurați-vă că datele cu caracter personal de pe acesta sunt **șterse complet**

- **Ștergeți datele cu caracter personal** de pe propriile dispozitive dacă s-a întâmplat cumva dintr-o necesitate să le stocați! O lipsă a ștergerii v-ar putea expune unor situații cu risc care, odată materializate, ar putea atrage amenzi asupra dumneavoastră!

Cazuistică relevantă

Un medic oncolog, în timp ce se află într-un autobuz aglomerat, primește rezultatele testelor unui pacient printr-un mesaj text pe telefonul său personal. Medicul decide să răspundă imediat pacientului, furnizându-i informații despre rezultatele testelor și recomandări pentru tratament. În același timp, medicul discută cu un coleg de muncă, prin intermediul aplicației WhatsApp, despre un caz dificil de diagnosticat și împărtășește detalii despre starea pacientului, inclusiv istoricul medical și simptomele.

Aceste acțiuni reprezintă o serie de rele practici:

- Utilizarea telefonului personal pentru comunicarea cu pacienții și colegii de muncă în legătură cu informații medicale confidențiale, fără a lua măsuri adecvate de securitate
- Discutarea detaliilor pacienților și a informațiilor lor medicale într-un loc public și aglomerat, unde persoane neautorizate pot asculta sau vedea ecranul telefonului
- Utilizarea unei aplicații de mesagerie chiar și criptată, cum ar fi WhatsApp, pentru a discuta despre cazuri medicale și a împărtăși informații personale ale pacienților

Aceste acțiuni expun pacienții și unitatea medicală la riscuri de confidențialitate și securitate a informațiilor personale. În cazul în care astfel de practici sunt descoperite și investigate de autoritatea de supraveghere, medicul și unitatea medicală ar putea fi supuși unor sancțiuni, inclusiv amenzi, pentru încălcarea prevederilor privind protecția datelor cu caracter personal.

Exemplu de utilizare inadecvată a tabletei / laptopului personal în cabinetul medical / spital:

Un medic dermatolog folosește tableta personală pentru a face poze la diverse leziuni ale pielii pe care le întâlnește la pacienții săi, pentru a le putea studia ulterior sau pentru a cere părerea unui coleg. Într-o zi, medicul uită tableta în sala de așteptare și un pacient, curios, navighează prin galeria de poze, întâlnind numeroase imagini cu leziuni ale pielii altor pacienți, unele dintre acestea fiind suficient de distinctive pentru a putea identifica pacientul în cauză.

Această situație reprezintă o încălcare majoră a GDPR, întrucât confidentialitatea pacienților a fost încălcată și datele cu caracter personal au fost expuse fără consimțământul acestora.

Exemplu cu ceasuri / brățări care colectează diverși parametri medicali:

Un medic cardiolog recomandă pacienților săi să utilizeze o brățară inteligentă care monitorizează ritmul cardiac și alți parametri esențiali. Aceste date sunt automat sincronizate cu un sistem online, la care medicul are acces. Într-o zi, sistemul online este compromis în urma unui atac cibernetic și datele tuturor pacienților sunt expuse pe internet.

În acest caz, medicul și instituția medicală ar putea fi considerați responsabili pentru încălcarea GDPR întrucât nu au asigurat securitatea adecvată a datelor colectate. În plus, dacă pacienții nu au fost informați corespunzător și nu și-au dat consimțământul în mod explicit pentru această colectare și procesare a datelor, aceasta constituie o altă încălcare a GDPR.

Cazuistică din activitatea Autorității de Supraveghere:

O amendă aplicată de Autoritatea pentru Protecția Datelor din Brandenburg:

O asistentă medicală de la un cabinet medical a stocat numărul de telefon al unei paciente în telefonul ei mobil și apoi a contactat-o în scopuri private. Acest aspect a fost reclamat de persoană și Autoritatea a aplicat o amendă de patru cifre.

Sursa: *Tätigkeitsbericht Datenschutz der LDA Brandenburg für das Jahr 2020*

3.7 ORIENTĂRI CU PRIVIRE LA UTILIZAREA E-MAILULUI ȘI FAXULUI

- Prezentarea unora dintre riscurile și problematicile asociate utilizării e-mailului și faxului în contextul desfășurării activității medicale

- Identificarea aspectelor cheie care pot fi luate în considerare pentru a transmite date cu caracter personal prim e-mail sau fax

!NB - Medicii sunt responsabili cu reducerea riscurilor asociate comunicării prin e-mail sau fax și cu asigurarea măsurilor de protecție rezonabile pentru a proteja informațiile medicale personale.

Care sunt riscurile?

Orice comunicare cu pacientul prin intermediul e-mailului și faxului pentru a-i transmite informații medicale, respectiv date cu caracter personal, poate genera uneori efecte negative în ceea ce privește protejarea drepturilor pacientului. Acest lucru poate include dificultăți cu privire la confirmarea identității pacientului, a aparținătorilor, asupra confirmării stării de sănătate a pacienților sau poate chiar genera plângeri și acțiuni în justiție.

Exemplu: lipsa transmiterii unei scrisori medicale de transfer poate lipsi pacientul de posibilitatea de a beneficia în timp util de servicii medicale.

Astfel, putem identifica următoarele problematici:

Confirmarea identității pacientului / aparținătorului într-un e-mail sau fax primit

Exemplu: ne contactează pe email o persoană care se declară aparținătorul pacientului Dan Ioan, de pe o adresă de tipul pisycutza1989@yahoo.com

Exemplu: transmitem pe email niște rezultate medicale către un destinatar de tipul dan.ioan@gmail.com în loc să trimitem către un destinatar de tipul ioan.dan@gmail.com.

Folosirea unor emailuri personale în desfășurarea activității profesionale

Exemplu: Medicul Ionescu Andrei își pune la dispoziția pacienților adresa de email ionescu.andrei1989@yahoo.com pentru a-i comunica date cu privire la istoricul medical și diverse documente specifice în acest sens. Această adresă este mai apoi folosită în mod abuziv de un pacient care încearcă să îi vândă aparatură medicală medicului.

Putem identifica și următoarele riscuri pentru pacienți:

Consecințe negative asupra sănătății dacă este vorba de o problemă ce necesită consultație imediată și totuși există o întârziere în timpul de răspuns

Interpretarea eronată a conținutului unui e-mail sau al unui fax, ceea ce ar putea duce la:

- consecințe negative asupra sănătății
- plângeri
- acțiuni în justiție dacă percepția pacientului este una de comunicare inadecvată sau ineficientă.

Utilizarea e-mailului pentru a comunica cu pacienții sau cu furnizorii terți de servicii medicale poate da naștere la următoarele probleme de confidențialitate și securitate:

Un mesaj transmis prin e-mail care nu este criptat poate fi:

- interceptat de către terți neautorizați (ex. hackeri); A se avea în vedere încheierea de contracte de servicii de întreținere a sistemelor software prin care personalul cu pregătire IT vă poate oferi sprijinul necesar.

E-mailurile care conțin date cu caracter personal pot fi interceptate de terți neautorizați dacă e-mailul este:

- transmis către o adresă greșită;
- trimis sau primit din locații nesecurizate, cum ar fi cele accesibile publicului (ex. te afli într-un restaurant care are conexiune liberă Wifi)

Atașamentele dintr-un e-mail pot conține viruși care ar putea provoca daune grave sistemelor informatice

- **Exemplu**: Un atașament prin care se transmite o felicitare electronică cu ocazia sărbătorilor conține un virus care, odată ajuns pe dispozitivul dumneavoastră, blochează complet accesul la date.

Datele personale de sănătate trimise prin e-mail pot părăsi spațiul României sau al Uniunii Europene în timpul transmiterii și pot face obiectul legilor din alte jurisdicții care au protecții inadecvate sau nu au nicio protecție.

- **Exemplu**: În calitate de medic, dorești să consulți opinia medicală a unui fost coleg de facultate angajat al unui spital din S.U.A. În acest sens îi trimiți pe emailul de serviciu un email cu analizele medicale (ex. o radiografie) a unui pacient. Astfel se realizează un transfer de date în afara U.E. în lipsa unor măsuri tehnice și organizatorice adecvate.

Transmiterea prin fax a informațiilor personale de sănătate poate prezenta riscuri de confidențialitate și de securitate, deoarece informațiile personale pot fi accesate de terți neautorizați dacă faxul este:

- trimis la un număr de fax incorect (din cauza unei greșeli de apelare sau a apăsării unei taste de apelare rapidă greșite);
- expus persoanelor neautorizate din simplul motiv că faxul este amplasat într-o locație deschisă, nesecurizată; sau
- accesate de terți care interceptează sau monitorizează transmisia.

Cele mai bune practici

Măsuri care pot ajuta la protejarea e-mailurilor împotriva interceptării:

Folosirea unei conexiuni securizate la internet (HTTPS): Când accesați contul dvs. de e-mail sau când trimiteți sau primiți e-mailuri este important să utilizați o conexiune securizată la internet (HTTPS). Acest lucru poate fi verificat prin prezența unei **săgeți verzi** sau a unui **semn de încuietoare** în bara de adrese a browserului dvs.

- **Utilizarea exclusivă a conturilor profesionale,** e-mailurilor profesionale, dispozitivelor de servicii fax aparținând operatorului și care îl identifică pe operator, destinate în mod specific unor tipuri de comunicări.

- **Activarea autentificării în doi pași**: Autentificarea în doi pași presupune introducerea a două informații de autentificare pentru a accesa un cont, cum ar fi o parolă și un cod de verificare trimis prin SMS sau prin aplicație. Această măsură de siguranță adițională poate face mai greu pentru un atacator să acceseze contul dvs. de e-mail.

- **Utilizarea unui software anti-virus actualizat**: Un software anti-virus actualizat poate detecta și preveni instalarea de software malițios pe dispozitivul dvs., cum ar fi virusuri sau spyware care ar putea intercepta e-mailurile dvs.

- **Evitarea conectării la rețele Wi-Fi publice nesecurizate**: Conectarea la rețele Wi-Fi publice nesecurizate poate fi periculoasă, deoarece un atacator ar putea intercepta orice informație transmisă prin intermediul acestora, cum ar fi e-mailurile.

- **Folosirea parolelor puternice**: Parolele puternice sunt mai dificil de ghicit sau de spart decât parolele simple. Este important să utilizați parole puternice pentru conturile dvs. de e-mail și să le schimbați frecvent.

- **Evitarea deschiderii de fișiere atașate sau link-uri suspecte în e-mailuri:** E-mailurile sunt adesea utilizate pentru a răspândi malware sau pentru phishing. Este important să fiți precauți atunci când deschideți fișiere atașate sau link-uri în e-mailuri, mai ales dacă provin de la expeditori necunoscuți sau neașteptați.

Păstrarea e-mailurilor sau a documentelor transmise prin fax

Pentru păstrarea / salvarea e-mailurilor și faxurilor vă rugăm să aveți în vedere următoarele aspecte:

- Nu faceţi sau reţineţi mai multe copii ale comunicărilor prin email decât este necesar;
- Distrugeţi în siguranţă copii suplimentare care nu mai sunt necesare (pentru fax sau e-mailurile printate)

Cazuistică relevantă

Un exemplu problematic ar putea fi următorul:

La sfârșitul programului de muncă, doriți să trimiteți un email care cuprinde date cu caracter personal în conținutul acestuia dar și în atașament, date precum nume, prenume, boli asociate, diagnostic. Acest email ar trebui trimis către 2 destinatari. Funcția de autocompletare a emailului adaugă un alt destinatar cu nume similar decât cel relevant pentru dumneavoastră. Nu observați acest lucru și trimiteți emailul. Tocmai s-a realizat o divulgare de date neautorizată. Putem vorbi despre un incident care pune în pericol confidențialitatea datelor persoanei respective.

Pentru a evita astfel de incidente care pun în pericol confidențialitatea datelor cu caracter personal și se încadrează în categoria divulgării neautorizate, vă recomandăm următoarele măsuri:

- **Verificarea Destinatarilor**: Întotdeauna verificați cu atenție adresele de email ale destinatarilor înainte de a trimite un email. Aceasta este o etapă importantă, mai ales atunci când funcția de autocompletare a emailului este activată.
- **Setarea Confirmării de Trimitere**: Majoritatea clienților de email au o funcție care solicită o confirmare înainte de a trimite un email. Activarea acestei funcții vă poate ajuta să verificați din nou destinatarii și conținutul înainte de a trimite emailul.
- **Atașamentele Criptate**: Atunci când trimiteți informații sensibile ca atașamente, considerați utilizarea criptării (parolării) acestora. Acest lucru poate ajuta la prevenirea accesului neautorizat în cazul în care emailul este trimis greșit.
- **Educarea Personalului**: Asigurați-vă că toți membrii echipei dumneavoastră sunt conștienți de importanța securității datelor și cunosc cele mai bune practici pentru trimiterea emailurilor. O formare adecvată poate reduce semnificativ riscul de eroare umană.

Aceste măsuri, luate împreună, pot reduce semnificativ riscul unei divulgări neautorizate de date cu caracter personal. Cu toate acestea, este important să rețineți că nicio măsură de securitate nu este perfectă, iar atenția și vigilența constantă sunt esențiale pentru protejarea datelor.

Cazuistică din activitatea Autorității de Supraveghere:

În noiembrie 2022, Autoritatea Națională de Supraveghere a finalizat o investigație la Medicover S.R.L., constatând încălcarea articolelor 32(4), 32(1) (b) și 32(2) din GDPR. Ca urmare, operatorul a fost amendat cu 4.901 RON (aproximativ 1.000 de euro). Investigarea a început după ce Medicover a notificat autoritatea despre o încălcare a securității datelor, conform articolului 33 din GDPR. Încălcarea a avut loc când un e-mail conținând acte adiționale ale contractelor de prestări servicii medicale ale altor clienți a fost trimis unui client în mod eronat. Aceasta a dus la pierderea confidențialității datelor cu caracter personal, cum ar fi nume, CNP, adrese și semnături. Autoritatea a constatat că Medicover nu a implementat măsuri tehnice și organizatorice adecvate pentru a asigura un nivel corespunzător de confidențialitate și securitate, conform articolului 32 din GDPR.
Sursa:
https://www.dataprotection.ro/page=Comunicat_Presa_24_11_2022&lang=ro

3.8 ORIENTĂRI PRIVIND PROTEJAREA DATELOR ÎN AFARA SEDIULUI PROFESIONAL OBIȘNUIT DE DESFĂȘURARE A ACTIVITĂȚII

Prezentarea bunelor și relelor practici și oferirea de recomandări cu privire la protejarea datelor în afara contextului profesional, precum conversațiile avute, documentele cu caracter medical, utilizarea dispozitivelor mobile personale și accesul la date medicale pe suport digital de acasă

Ce ar trebui să cunoașteți în materie de Bune practici:

Respectarea confidențialității în conversații: Discuțiile despre pacienți și informațiile lor medicale ar trebui să aibă loc într-un mediu privat și securizat. Nu este recomandat să se poarte astfel de discuții în locuri publice sau în prezența unor terțe persoane care nu au nevoie să cunoască aceste informații. Astfel:

- Evitați discuțiile în care sunt abordate informații medicale, personale ale unui pacient în zone publice, cum ar fi în lifturi, pe scări, în timpul călătoriilor cu mijloacele de transport în comun (tramvaie, metrou, tren, autobuz, taxi) sau avioane, în restaurante sau pe stradă.
- Totodată se recomandă evitarea utilizării telefoanelor mobile pentru a discuta despre starea de sănătate a unor pacienți în timp ce sunteți în tranzit (ex. metrou, tramvai) deoarece aceste convorbiri pot fi interceptate sau auzite.

Asigurarea confidențialității și securității documentelor fizice: Atunci când medicii utilizează înregistrări clinice pe hârtie în afara programului de lucru sau spațiului alocat desfășurării activității medicale specifice este important să urmeze bunele practici pentru a asigura confidențialitatea și securitatea informațiilor. În acest sens, medicii ar trebui:

- Să scoată înregistrările clinice în afara spațiului destinat desfășurării activității medicale specifice doar atunci când este absolut necesar pentru îndeplinirea îndatoririlor lor profesionale (ex. vizite la domiciliul pacienților sau consultări cu alți specialiști în afara sediului obișnuit)
- Să solicite aprobarea supervizorului înainte de a scoate înregistrările clinice din spațiul destinat desfășurării activității medicale, pentru a se asigura că există un motiv justificat pentru transportarea acestora
- Să lase originalele în spațiul destinat desfășurării activității medicale (cabinet) și să ia cu ei doar copii ale înregistrărilor, pentru a minimiza riscul de pierdere sau deteriorare a documentelor originale
- Să transporte doar cantitatea minimă de informații personale necesară pentru a efectua sarcina, evitând expunerea nejustificată a datelor pacienților
- Dacă înregistrările sunt voluminoase, să apeleze la serviciile unui curier cu care furnizorul de servicii medicale are relații contractuale care asigură cadrul de confidențialitate necesar (prin clauze contractuale) pentru transportul înregistrărilor în siguranță până la destinație
- Să utilizeze dosare care asigură un nivel ridicat de confidențialitate (ex. plicuri opace) păstrându-le sub control în permanență, inclusiv în timpul meselor și al pauzelor
- Atunci când lucrează de acasă, să păstreze înregistrările medicale blocate într-un sertar de birou sau într-un dulap pentru dosare, pentru a preveni accesul neautorizat al membrilor familiei, al prietenilor respectiv al altor persoane care nu au legătură cu activitățile profesionale
- În cazul în care transportă documente cu mașina, să le păstreze blocate în portbagaj înainte de începerea călătoriei, pentru a reduce riscul de furt
- Să evite examinarea înregistrărilor clinice în locuri publice, cum ar fi mijloacele de transport în comun, unde acestea pot fi văzute sau accesate de persoane neautorizate

- Să nu lase documentele la vedere nici chiar în camerele de hotel, acestea se pot depune în seiful camerei sau al hotelului pentru a asigura confidențialitatea acestora
- La întoarcerea în unitatea medicală, să returneze imediat înregistrările clinice la locul lor de depozitare original
- Să distrugă în mod sigur orice copii ale înregistrărilor care nu mai sunt necesare, pentru a preveni divulgarea neintenționată a informațiilor personale ale pacienților

Utilizarea dispozitivelor mobile personale: În contextul utilizării dispozitivelor portabile de către medici, inclusiv a dispozitivelor personale, este esențial să se acorde o atenție sporită securității și confidențialității informațiilor pacienților. Astfel, următoarele bune practici ar trebui să fie respectate:

- Medicii ar trebui să evite stocarea informațiilor personale ale pacienților pe dispozitivele electronice portabile, cu excepția cazului în care este absolut necesar pentru îndeplinirea sarcinilor lor profesionale
- Este esențial ca dispozitivele electronice portabile care conțin informații personale să fie protejate cu parole puternice. Se recomandă utilizarea unor metode sigure de autentificare, cum ar fi autentificarea în doi pași, pentru a acorda accesul utilizatorilor.
- Medicii trebuie să păstreze dispozitivele electronice portabile în locuri sigure, pentru a preveni pierderea sau furtul acestora (ex. sertare de birou, containere sau fișete asigurate cu sistem de închidere ori încăperi securizate). Dispozitivele ar trebui să rămână sub supravegherea unei singure persoane, inclusiv în timpul meselor și al pauzelor.
- Este important ca medicii să elimine în mod corespunzător informațiile personale sensibile care nu mai sunt necesare de pe dispozitivele electronice portabile (ex. laptopuri). În acest sens, se recomandă utilizarea unui program de ștergere digitală, în loc să se bazeze exclusiv pe funcția de ștergere, deoarece informațiile pot rămâne în continuare pe dispozitiv.
    - Un exemplu de program care poate fi folosit pentru a șterge în mod corespunzător informațiile personale sensibile de pe dispozitivele electronice este "Eraser". Eraser este un software gratuit și open-source care permite utilizatorilor să șteargă în mod sigur datele de pe hard disk, suprascriindu-le în mod repetat cu modele de date aleatoare, ceea ce face recuperarea datelor aproape imposibilă. Acest program este compatibil cu majoritatea sistemelor de operare Windows și este recunoscut pentru fiabilitatea și eficiența sa.

Accesul la date medicale pe suport digital de acasă: În contextul lucrului de acasă, medicii și personalul medical trebuie să ia în considerare aspectele de securitate privind accesul și gestionarea înregistrărilor care conțin date medicale ale pacienților pe computere personale, laptopuri sau dispozitive electronice portabile. Iată câteva bune practici pentru a aborda riscurile de securitate:

- Asigurați-vă că autentificarea pentru accesarea informațiilor personale este protejată cu parolă și nu permiteți dispozitivului să salveze parolele.
- Utilizați funcția: Deconectare (log off) atunci când nu utilizați computerul sau laptopul și setați o deconectare automată după o perioadă de inactivitate.
- În funcție de riscurile de securitate la securitatea fizică ce pot apărea păstrați computerele de acasă într-o cameră cu acces restricționat.
- Asigurați-vă că dispozitivele de acasă au cel puțin un firewall personal, protecție antivirus și protecție anti-spyware instalate.
- Instalați actualizări și patch-uri de securitate în mod regulat pentru a vă asigura că dispozitivele sunt protejate.
- Folosiți o conexiune criptată cu rețeaua gazdă, cum ar fi o rețea privată virtuală (VPN), pentru a accesa informații personale de la distanță.
- Fiți conștienți de "spionajul peste umăr" și evitați ca membrii familiei sau prietenii să observe ecranul computerului de acasă.

Ce ar trebui să cunoașteți în materie de Rele practici:

Divulgarea neintenționată a informațiilor: Discuțiile despre pacienți și informațiile lor medicale în locuri publice sau în prezența unor terțe persoane neautorizate pot duce la încălcarea confidențialității și, în consecință, la încălcarea unor drepturi ale pacientului, în special a dreptului la viață privată.

Lipsa securizării documentelor cu caracter medical: Păstrarea documentelor medicale în locuri accesibile altor persoane sau neimplementarea măsurilor de securitate adecvate pentru documentele digitale pot duce la furtul, pierderea sau divulgarea neautorizată a datelor cu caracter personal ale pacienților.

- **Utilizarea dispozitivelor mobile personale fără măsuri de securitate adecvate**: Accesarea datelor medicale sau comunicarea cu pacienții folosind dispozitive mobile personale neprotejate poate duce la compromiterea datelor și la posibile încălcări ale GDPR.

- **Accesul neautorizat la date medicale pe suport digital de acasă**: Accesul la datele medicale fără a urma îndrumările clare ale unității medicale, respectiv bunele practici, poate duce la încălcarea GDPR și la posibile amenzi.

Cazuistică relevantă

În timpul concediului său, un medic se întâlnește cu un vechi prieten care îi cere informații despre starea de sănătate a unui pacient comun, crezând că medicul ar putea să îl ajute. Medicul, fără să aibă în vedere posibilele consecințe ale acțiunilor sale, îi oferă prietenului detalii despre diagnosticul și tratamentul pacientului.

Ulterior, prietenul discută aceste informații cu alte persoane, iar informația ajunge la urechile pacientului, care nu și-a dat consimțământul pentru divulgarea datelor sale medicale. Această situație constituie o încălcare a confidențialității și o breșă în conformitate cu GDPR, care poate duce la sancțiuni, inclusiv amenzi, pentru medicul în cauză.

Cazuistică din activitatea Autorității de Supraveghere:

Autoritatea franceză pentru protecția datelor (CNIL) a aplicat amenzi de 3000 și de 6.000 euro către doi medici pentru încălcarea articolelor 32 și 33 din GDPR. Medicii au stocat date de imagini medicale, cum ar fi imagini RMN și cu raze X, precum și date personale ale pacienților săi, precum nume, date de naștere și detalii despre tratamentele lor, pe niște servere pentru a le putea accesa de pe calculatoarele personale de acasă.

Analiza sistemelor a relevat că accesul la servere nu era securizat corespunzător, permițând astfel accesul neautorizat la datele pacienților. S-a constatat că această breșă de securitate exista de aproximativ cinci ani și nu a fost raportată la Autoritate. Drept urmare, autoritatea de protecție a datelor a concluzionat că medicul nu a implementat măsurile tehnice și organizatorice adecvate pentru a asigura securitatea datelor personale ale pacienților săi. Sursa: *https://www.studiolegalestefanelli.it/en/european-data-protection-observatory*

3.9 ORIENTĂRI PRIVIND FURNIZAREA DE SERVICII DE TELEMEDICINĂ

Explorarea unor bune și unor rele practici în ceea ce privește confidențialitatea, securitatea, stocarea și accesul datelor în domeniul telemedicinii

Telemedicina a devenit tot mai populară în ultimii ani, oferind acces la servicii medicale pentru pacienți din zone îndepărtate sau cu mobilitate redusă. Cu toate acestea, furnizarea acestor servicii implică prelucrarea unor cantități mari de date cu caracter personal și sensibil, ceea ce ridică preocupări legate de protecția datelor, confidențialitatea și securitatea acestora.

Telemedicina poate fi utilizată de la o clinică ce furnizează un astfel de serviciu la domiciliu, de la o clinică la o altă clinică, de la domiciliul medicului la domiciliul pacientului și de la o clinică la o comunitate (ex: o societate de îngrijiri specifice unei categorii de pacienți).

Potrivit unui studiu american, **principalele metode de livrare pentru telemedicină** includ aplicațiile sau serviciile specializate pentru telemedicină (73%); aplicații sau servicii non-telemedicină, cum ar fi Zoom, FaceTime; video (59%); portalul pacientului, cum ar fi mesageria și e-mailul securizat (52%); și telefon (49%). Instrumentele tehnologice utilizate în mod obișnuit pentru telemedicină includ conexiune la internet de mare viteză, camere web, tablete, laptopuri, telefoane mobile, software, stații de lucru la domiciliu etc.

Elementele care pot influența confidențialitatea și securitatea datelor pot fi grupate în 3 categorii: **elemente de mediu, tehnologice și operaționale.**

Elementele de mediu se referă la ceea ce se află împrejurul pacientului la momentul consultației, condițiile de viață și conexiunile sociale - care au un impact direct sau indirect asupra protecției confidențialității și securității.

Populațiile vulnerabile, cum ar fi persoanele fără adăpost, vârstnicii, adolescenții, părinții și pacienții cu probleme de sănătate mintală sunt adesea afectați/îngrijorați de lipsa spațiului privat pentru vizitele virtuale. Vizitele de telemedicină au arătat dificultăți în împărtășirea informațiilor sensibile de sănătate pentru pacienții cu HIV/SIDA, probleme de comportament sau de sănătate mintală, precum și discuții despre contraceptive pentru pacienții adolescenți.

A avea încredere în furnizori și în alți lucrători din domeniul sănătății atunci când partajați informații sensibile reprezintă adesea o provocare și un deziderat.

Un alt punct de vedere al confidențialității este că locația videoconferinței poate expune din neatenție detalii despre condițiile de viață ale pacientului, spațiul, locația etc.

Elementele de tehnologie includ probleme de securitate a datelor, cum ar fi piratarea vizitelor video, accesul limitat la internet și tehnologie, lipsa dispozitivelor digitale, utilizarea datelor celulare sau Wi-Fi publice, lipsa de alfabetizare digitală - evidențiată prin cunoștințele limitate sau înțelegerea limitată a tehnologiei utilizate, calitatea slabă a rezultatului audio sau video.

O altă problemă cu tehnologia de telemedicină este înțelegerea utilizării acesteia și alfabetizarea digitală, factori care pot limita calitatea evaluărilor sau diagnosticarea unei suferințe.

Elementele operaționale pot face referire la formarea și educația adecvată atât pentru personal, cât și pentru furnizori.

Ce ar trebui să cunoașteți în materie de Bune practici:

Implementarea unor măsuri de securitate adecvate: Este esențial să se implementeze măsuri de securitate adecvate pentru a proteja datele cu caracter personal ale pacienților în cadrul telemedicinii. Aceasta include criptarea datelor de pe dispozitive (ex. parole puternice), autentificarea în doi factori pentru accesul la sistemele informatice (de regulă se poate realiza din setări) și actualizarea periodică a sistemelor folosite (actualizări ale sistemelor de operare).

Stocarea și accesul la date: Un aspect deosebit de important este următorul:

Unde stocăm datele? Dacă înregistrăm prin aplicațiile specifice discuțiile avute cu pacienții, acestea unde vor fi stocate? (pe un hard-disk extern? La un furnizor de servicii de cloud?)

În domeniul medical, datele pacienților sunt adesea sensibile și trebuie să fie protejate conform regulilor stricte de confidențialitate și conform GDPR.
Aici sunt câteva opțiuni de stocare a datelor:

- **Stocarea pe Cloud:** Cloud-ul oferă flexibilitate și accesibilitate. Poți accesa datele de oriunde și oricând. Mulți furnizori de servicii de cloud oferă, de asemenea, opțiuni avansate de securitate și criptare. Cu toate acestea, trebuie să te asiguri că furnizorul de cloud respectă regulile GDPR și că datele sunt stocate într-o manieră securizată. Exemple de astfel de furnizori pot fi Microsoft Azure, Amazon Web Services (AWS) sau Google Cloud.

- **Hard-Disk Extern:** Un hard-disk extern poate fi o opțiune bună dacă dorești să ai controlul total asupra datelor tale. Totuși, aceste dispozitive pot fi vulnerabile la furt, pierdere sau deteriorare fizică. Este important să asiguri criptarea datelor stocate pe hard-disk-uri externe și să ai un plan de backup pentru cazul în care dispozitivul este pierdut sau deteriorat.

- **Stocarea Locală în Rețea** (Network Attached Storage - NAS): Acest tip de stocare implică utilizarea unui dispozitiv de stocare conectat la rețeaua ta locală. NAS-urile pot fi configurate pentru a oferi niveluri ridicate de securitate și redundanță. Sunt, de asemenea, o opțiune bună pentru stocarea datelor la nivel de echipă sau organizație.

Indiferent de opțiunea aleasă, este esențial să ai o strategie solidă de backup a datelor. Acest lucru poate implica backup-uri regulate pe cloud, pe hard-disk-uri externe sau pe alte dispozitive de stocare. O strategie de backup bine gândită poate ajuta la prevenirea pierderii de date în cazul unui incident neașteptat.

Cât timp stocăm datele după furnizarea serviciului? (spre exemplu: se șterg imediat? se pun la dispoziția clientului în copie și se păstrează pentru o perioadă de 3 ani?)

În ceea ce privește **durata de păstrare a datelor în contextul telemedicinei**, acest lucru ar trebui să se bazeze pe necesitatea medicală, pe reglementările legale relevante și pe principiile de bază ale GDPR. Potrivit GDPR, datele personale ar trebui să fie "păstrate într-o formă care permite identificarea persoanelor vizate pentru o perioadă care nu depășește perioada necesară în vederea îndeplinirii scopurilor pentru care sunt prelucrate datele personale". Acesta este cunoscut sub numele de **"principiul minimizării datelor".**

În plus, diferite țări pot avea reglementări specifice despre cât timp trebuie păstrate înregistrările medicale. De exemplu, în multe țări din Uniunea Europeană, înregistrările medicale trebuie păstrate pentru o perioadă minimă de 10 ani după ultima înregistrare. Astfel, de fiecare dată se va verifica termenul de păstrare stabilit de lege la nivelul României. În caz contrar, vom merge pe principiul general enunțat mai sus, care ar trebui să se reflecte într-un document de tip „nomenclator arhivistic” care să stabilească perioada concretă de păstrare a datelor.

Cum se asigură securizarea sistemelor de protecție? (acces la hard-disk îl are doar persoana cu atribuții specifice sau conducătorul unității medicale?).

Pentru aceasta se recomandă contractarea serviciilor de mentenanță a sistemelor informatice și realizarea de discuții specifice pentru fiecare sistem utilizat în parte.

Totodată, trebuie să se limiteze accesul la date doar la personalul autorizat și să se implementeze proceduri specifice prin care să monitorizăm și să documentăm accesul la datele cu caracter personal. În acest sens, dacă se dezvoltă o aplicație prin care se oferă servicii de telemedicină, este foarte relevant să stabilim clar rolurile persoanelor care se pot conecta: pacienți, registratori medicali, personal medical, echipa de IT care oferă mentenanță, echipa de management ș.a.

Accesul la date într-o aplicație de telemedicină trebuie să fie foarte bine reglementat și structurat în funcție de roluri pentru a respecta reglementările GDPR. Iată câteva recomandări generale:

- **Pacienții** ar trebui să aibă acces doar la propriile date medicale și istoricul lor medical. Aceștia ar trebui să poată corecta și actualiza propriile informații personale, dar nu ar trebui să poată accesa informațiile altor pacienți.

- **Registratorii medicali** ar trebui să aibă acces la datele pacienților în scopul înregistrării și gestionării programărilor. Ei ar trebui să poată vedea și modifica informații precum numele, adresa și datele de contact ale pacientului, dar accesul la informațiile medicale ar trebui să fie limitat.

- **Personalul medical** ar trebui să aibă acces la datele medicale ale pacienților pentru a putea furniza îngrijire medicală adecvată. Totuși, accesul ar trebui să fie limitat la pacienții de care se ocupă în mod direct.

- **Echipa de IT** ar trebui să aibă acces limitat la datele cu caracter personal, doar în măsura în care este necesar pentru realizarea lucrărilor de întreținere și rezolvarea problemelor tehnice. Ideal, accesul ar trebui să fie realizat într-un mod care nu permite vizualizarea datelor cu caracter personal.

- **Echipa de management** ar putea avea nevoie de acces la datele pacienților într-un format anonimizat sau agregat pentru analiza performanței, planificarea resurselor sau alte scopuri de management.

Pentru a monitoriza și documenta accesul la date, este important să se implementeze un sistem de jurnalizare care să înregistreze toate accesările și modificările datelor cu caracter personal. Acest jurnal de audit ar trebui să includă detalii precum cine a accesat datele, ce date au fost accesate, când au fost accesate și ce acțiuni au fost luate.

Respectarea drepturilor pacienților: Chiar dacă se primește un „simplu email” prin care se solicită lămuriri cu privire la datele prelucrate, la locația lor, la cine ar putea avea acces, la măsurile de securitate luate, este deosebit de important să tratăm aceste cereri cu responsabilitate! Astfel recomandăm să se contacteze imediat persoana pentru a îi aduce clarificările necesare.

Ce ar trebui să cunoașteți în materie de Rele practici:

- **Neglijarea securității datelor:** un caz relevant de jurisprudență este cel al Babylon Health (va fi menționat la finalul capitolului), în care pacienții au putut accesa înregistrări video ale consultațiilor altor pacienți din cauza unor deficiențe tehnice de securitate.

- **Stocarea inadecvată a datelor** care poate duce la acces neautorizat sau pierderea datelor cu caracter personal: un exemplu relevant este cazul unei companii de telemedicină care a stocat datele pacienților pe servere necriptate, expunându-le la riscul de a fi accesate sau interceptate de terțe părți neautorizate.

- **Nerespectarea drepturilor pacienților conform GDPR**, cum ar fi neîndeplinirea solicitărilor de acces, rectificare sau ștergere a datelor: un caz de jurisprudență evidențiază o companie de telemedicină care nu a răspuns în mod corespunzător solicitărilor pacienților de a-și accesa datele lor cu caracter personal, încălcând astfel drepturile acestora conform GDPR.

Cazuistică relevantă

Un exemplu de rea practică în domeniul telemedicinii este cazul unei clinici care utilizează o platformă de telemedicină pentru a comunica cu pacienții săi. Într-un caz particular, un angajat al clinicii, care nu avea responsabilități legate de protecția datelor sau accesul la informațiile pacienților, a reușit să acceseze în mod neautorizat înregistrările video ale consultațiilor unor pacienți. Angajatul a împărtășit apoi aceste înregistrări cu alte persoane, ceea ce a dus la încălcarea confidențialității și a drepturilor pacienților.

Această situație reprezintă o rea practică în telemedicină deoarece clinica nu a asigurat securitatea adecvată a datelor pacienților și nu a limitat accesul la aceste informații doar la personalul autorizat. Acest caz ilustrează importanța implementării unor măsuri de securitate adecvate și respectarea drepturilor pacienților în conformitate cu RGPD, pentru a evita sancțiuni și eventuale amenzi.

Cazuistică din activitatea Autorității de Supraveghere:

Babylon Health: Compania a avut un incident de securitate în 2020, în care pacienții au putut accesa înregistrări video ale consultațiilor altor pacienți. Information Commissioner's Office (ICO) – autoritatea de supraveghere din Marea Britanie - a investigat incidentul și a emis un avertisment către companie pentru a remedia deficiențele de securitate.

Sursa: *BBC News, știre din 9 iunie 2020: https://www.bbc.com/news/technology-52986629*

Doctolib: Autoritatea franceză de protecție a datelor (CNIL) a amendat Doctolib cu 50.000 de euro în octombrie 2020 pentru încălcarea GDPR. CNIL a identificat probleme legate de stocarea inadecvată a datelor pacienților și lipsa de securitate a datelor, precum și utilizarea de cookie-uri fără acordul prealabil al utilizatorilor.

Sursa: *Le Monde Informatique: https://www.lemondeinformatique.fr/actualites/lire-cnil-doctolib-epingle-sur-le-rgpd-80510.html*

3.10 ORIENTĂRI PRIVIND GESTIONAREA CERERILOR PERSOANELOR VIZATE (PACIENȚI / APARȚINĂTORI) CU PRIVIRE LA PROPRIILE INFORMAȚII

- Explicarea drepturilor persoanelor vizate (pacienți / aparținători / persoane cărora li se prelucrează datele cu caracter personal) de a avea acces la propriile date

- Identificarea aspectelor ce trebuie să fie luate în considerare atunci când se pregătește răspunsul

- Prezentarea posibilităților de răspuns, termenele limită, excepțiile de la comunicare și aspecte tehnice și organizatorice

Regulamentul General privind Protecția Datelor (R.G.P.D.) oferă **drepturi sporite persoanelor vizate** (pacienți, aparținători, medici, sau alte persoane fizice cu care se interacționează) sens în care operatorul trebuie să se asigure că le respectă.

Practicile impun anumite **eforturi rezonabile operatorului** cu privire la transmiterea informațiilor relevante. Între acestea vom găsi în continuare punctate cele mai importante aspecte.

Exercitarea drepturilor

Atunci când o persoană dorește să afle mai multe despre propriile date poate depune o cerere în acest sens:

- la adresa de corespondență a operatorului
- pe email
- în alt format care poate fi documentat (ex. audio-video)

Pentru o eficientizare a organizării muncii și răspunsurilor a se vedea **Anexa 5 Formularul tip cerere de acces la datele cu caracter personal.**

Cel mai adesea obiectul cererilor va fi:

- **de a fi informat** – adică să știe ce date îi sunt prelucrate
  - Exemplu: Pacientul X poate să citească într-o notă de informare pusă la dispoziție de către un spital despre datele care îi sunt prelucrate.
- **de acces** – să primească acces la propriile date (ex. copii după analize medicale)
  - Exemplu: Sunt pacientul X, vă rog să îmi trimiteți o copie electronică a tuturor analizelor realizate pe durata internării
- **de ștergere** – să fie șters din bazele de date (ex. cazul abonării la buletine informative periodice care sunt trimise de operator)
  - Exemplu: Sunt pacientul X, sunt deosebit de deranjat de comunicările dumneavoastră. Vă rog să mă ștergeți din orice fel de bază de date!

Ce ar trebui să cunoașteți:

Faptul că există excepții: Nu întotdeauna trebuie să dăm răspuns afirmativ cererilor!

- Dacă există o obligație legală de păstrare a datelor (ex. 5 ani) nu vom putea da curs unei solicitări prin care ni se cere să ștergem toate datele din sistemul de gestiune a pacienților, pe motiv că pacientul nu mai dorește să aibă contact cu spitalul, fiind nemulțumit de serviciile medicale ale acestuia.

- Nu comunicăm date atunci când acestea duc la o dezvăluire a datelor altei persoane, întrucât ar putea provoca un prejudiciu grav sănătății sale psihice, fizice sau de altă natură! Exemplu: accesul la camerele de supraveghere video din saloanele de terapie intensivă.
    - *Pot exista totuși profesioniști sau instanța de judecată care sunt îndreptățiți să aibă acces la aceste date foarte sensibile, însă datele trebuie prelucrate având un temei legal, scop specific și garanții de protecție a datelor.*

Termenul de răspuns este de **o lună** de la data primirii solicitării! Acest termen poate fi prelungit până la 3 luni dacă se justifică depunerea unor eforturi deosebit de mari pentru pregătirea răspunsului, însă oferind un răspuns prealabil de informare din partea operatorului:

- **Exemplu de răspuns**: *... Am primit solicitarea dumneavoastră și a fost dată în lucru colegilor noștri. Întrucât se impun verificări numeroase ale bazelor de date, vom reveni cu un răspuns către dumneavoastră cel târziu până la data de ...* .

Un număr mare de cereri cu obiect identic, de la aceeași persoană, îndreptățește operatorul să impună o taxă pentru oferirea răspunsului.

- Justificarea rezidă în costurile reale pentru pregătirea și transmiterea răspunsurilor. În acest calcul se iau în considerare: numărul de persoane implicate în procesul de răspuns, numărul de ore alocate, pregătirea materialelor – printare, înregistrare și alte operațiuni organizatorice, cheltuieli de expediere – curierat ș.a.

- În acest caz, se va transmite de către operator o estimare a costurilor pe care persoana o poate plăti integral sau parțial. Costul ridicat nu se justifică de regulă, deoarece poate conduce la împiedicarea indirectă a dreptului.

Este foarte indicat să avem o **procedură de răspuns la cereri și formulare standardizate** după care răspundem.

- Pentru a vă ajuta, vă punem la dispoziție un model de procedură de lucru (**Anexa 6 Model de procedură de soluționare a cererilor persoanelor vizate**) și model de formulare (**Anexa 7 Model de formular de răspuns la cererile persoanei vizate**).

Important de știut!

Nu putem comunica date oricui despre oricine! Problema cea mai mare este a „presupușilor” aparținători care cer informații despre pacienți! În acest sens trebuie să ținem cont de necesitatea identificării reale a aparținătorului.

S-ar putea ca **aparținătorul să fie sau să nu fie declarat** (prin formularele specifice) **de către pacient**. S-ar putea petrece o situație în care nu avem pe nimeni declarat ca aparținător, însă se impun comunicări urgente cu membrii de familie care țin de viața sau de sănătatea persoanei!

În nici un caz **nu putem refuza dreptul aparținătorilor pacientului respectiv de a fi informați** cu privire la starea de sănătate a acestuia însă, atunci când se primesc astfel de cereri, se impun minime diligențe din partea personalului angajat care să poată identifica aparținătorul și dacă este posibilă transmiterea sau nu a datelor.

În trecut au fost numeroase cazuri de **divulgare de date către așa-zișii aparținători**, care în fapt erau jurnaliști sau persoane neautorizate să primească acces la date, astfel operatorul ar putea să aibă parte de un incident la adresa confidențialității datelor, riscând să i se atragă sancțiuni.

Între **bunele practici** care se recomandă se numără următoarele:

- Să fie oferite informații în primă fază doar **rudelor de gradul I și gradul II**, dacă pacientul nu a refuzat în scris această acțiune
- Accesul la date prin telefon **să se rezume la telefonul operatorului** / secției / dedicat activității
    - Ar fi indicat să existe o **procedură de identificare a persoanelor prin telefon, dar și a relației cu pacientul.** Spre exemplu să se adreseze două trei întrebări de verificare înainte de a se oferi informații referitoare la starea de sănătate a pacientului.
    - **Fără a avea certitudinea identității interlocutorului oferim doar date limitate despre evoluția pacientului**, generale (“este constient, cooperant, orientat, se simte mai bine” etc), fără a oferi date privind diagnostic, intervenție chirurgicală ș.a. până în momentul identificării certe a solicitantului

- În privința emailului, **cererile de acces trebuie să fie adresate conturilor de email oficiale ale operatorului și se va răspunde de pe canalele oficiale de comunicare** (adresa de email a secției sau a registraturii sau a Responsabilului cu Protecția Datelor)

Cazuistică relevantă

Un jurnalist s-ar putea prezenta ca fiind un membru al familiei pacientului și ar putea solicita informații despre starea de sănătate a acestuia. Dacă personalul spitalului oferă aceste informații fără a verifica identitatea și relația jurnalistului cu pacientul, acest lucru constituie o încălcare a confidențialității datelor pacientului și a dispozițiilor GDPR.

Pentru a evita astfel de situații, este important ca personalul să urmeze bunele practici de verificare a identității și relației persoanei care solicită informații, să asigure comunicarea doar prin canalele oficiale și să respecte procedurile interne de răspuns la cererile de acces la datele personale.

Cazuistică din activitatea Autorității de Supraveghere:

Autoritatea Națională de Supraveghere a finalizat o investigație în 2021 la operatorul **Actamedica SRL** și a constatat încălcări ale prevederilor GDPR. Ca urmare, Actamedica SRL a fost sancționat cu amenzi de 9.836,6 lei (2.000 EURO) pentru încălcarea art. 28 alin. (1) și art. 32 și de 4.918,3 lei (1.000 EURO) pentru încălcarea art. 33. Un avertisment a fost dat și pentru încălcarea:

- Articolul 12 alineatul (3) se referă la obligația operatorului de date de a furniza informațiile solicitate de persoana vizată în legătură cu prelucrarea datelor sale personale într-un termen rezonabil, dar în orice caz în termen de o lună de la primirea solicitării.
- Articolul 15 alineatul (1) se referă la dreptul persoanei vizate de a obține de la operatorul de date confirmarea că datele sale personale sunt sau nu prelucrate și, în caz afirmativ, acces la informațiile despre datele personale și detalii suplimentare, cum ar fi scopul prelucrării, categoriile de date personale implicate, destinatarii sau categoriile de destinatari cărora le-au fost sau le vor fi dezvăluite datele personale, perioada de stocare, dreptul de a solicita rectificarea sau ștergerea datelor personale, dreptul de a depune plângere la o autoritate de supraveghere și informații disponibile despre sursa datelor, dacă acestea nu au fost colectate direct de la persoana vizată.

Investigația a început după o plângere care reclama faptul că Actamedica SRL a informat o persoană fizică despre pierderea probelor sale biologice și a unei sume de bani trimise prin curierat. Persoana fizică a solicitat informații despre ce date personale i-au fost expuse și dacă ANSPDCP a fost notificată, dar operatorul nu a oferit un răspuns adecvat. În timpul investigației s-au constatat deficiențe în măsurile de securitate și nerespectarea art. 12 alin. (3) și 15 alin. (1), ceea ce a condus la aplicarea amenzilor și avertismentului menționate anterior.

Sursa: *https://www.dataprotection.ro/?page=Comunicat_Presa_24_08_2021&lang=ro*

3.11 ORIENTĂRI PRIVIND GESTIONAREA RECLAMAȚIILOR FORMULATE DE ANGAJAȚI, RESPECTIV DE PACIENȚI

- Prezentarea celor mai bune practici referitoare la situațiile în care medicul se confruntă cu reclamații sau plângeri specifice protecției datelor din partea angajaților sau pacienților

Prin drepturile oferite persoanelor vizate (angajați, colaboratori, pacienți sau alte persoane fizice cu care se interacționează) Regulamentul General privind Protecția Datelor caută să responsabilizeze operatorul (cabinetul, spitalul, clinica) privitor la felul în care gestionează datele persoanelor și se oferă persoanei vizate pârghiile juridice pentru a avea controlul asupra datelor sale.

În acest cadru, în mod frecvent, apar situații în care persoanele vizate își exprimă nemulțumiri referitoare la felul în care datele le-au fost gestionate.

Exemple de situații:

- Un medic dorește **să participe la un congres științific**, ocazie cu care prezintă o lucrare de specialitate în care se regăsesc detalii referitoare la inițialele numelui pacientului, vârsta, sexul, istoricul medical detaliat, proceduri medicale avute, spitalizări, diagnostic etc. Aceste informații permit uneori identificarea cu ușurință a persoanei și sunt informații sensibile. Aceasta face plângere la Autoritatea de Supraveghere (caz real de sancțiune din Ungaria).

Un alt medic **constituie un grup de Whatsapp cu pacienții săi** (230) pentru a comunica schimbarea adresei și a comunica aspecte referitoare la programări, consultări ș.a. O persoană se declară nemulțumită de faptul că 229 persoane i-au putut vedea numărul de telefon / fotografia. Autoritatea de Supraveghere constată lipsa consimțământului și aplică amendă medicului (caz real din Germania).

- Asigurați-vă că aveți consimțământul pacienților atunci când doriți să aveți astfel de comunicări pe grupuri de Whatsapp în care pot apărea și date cu caracter sensibil.

Medicul a recomandat niște **produse medicale** unui pacient ca parte a unui tratament. După câteva zile acesta a fost sunat de agenția care comercializa acel bun. Pacientul s-a declarat total nemulțumit acuzând medicul că ar fi trimis datele spre companie. Autoritatea de Supraveghere constată lipsa consimțământului pentru transferul de date și sancționează medicul (caz real din Italia).

- !NB - nu comercializați datele pacienților!

O unitate spitalicească ține un registru de evidență al persoanelor care sunt internate, cuprinzând în cadrul acestui registru și o rubrică în care se menționează dacă pacientul a efectuat vreo donație către fundația spitalului. Aceasta este o practică extrem de greșită, deoarece creează aparența că serviciile spitalului sunt influențate faptic de existența vreunei donații din partea pacientului. Chiar dacă actul donației se bazează pe consimțământ, în realitate un asemenea consimțământ nu îndeplinește condiția de a fi liber exprimat.

Ce ar trebui să cunoașteți:

Faptul că există uneori situații cu privire la care persoanele vizate își pot exercita drepturile și să aibă solicitări îndreptățite, cum ar fi: să aibă acces la datele proprii, să fie informați, să li se rectifice datele sau să aibă drept de opoziție și ștergere. În fiecare dintre aceste situații este bine să reacționăm cu **maximă promptitudine și cordialitate**. Lipsa unui răspuns în termen de o lună la o plângere adresată (pe e-mail, spre exemplu) poate atrage sancțiuni mari chiar pentru faptul că nu i s-a răspuns persoanei.

- În multe dintre cazuri **persoanele au o altă nemulțumire decât cea legată de protecția datelor** însă se folosesc de o neregularitate sesizată pentru a sancționa sau a pedepsi operatorul sau medicul. Identificați în mod real care este nemulțumirea și încercați să o soluționați în primul rând pe aceea. O simplă aducere la cunoștință a unor neconformități identificate în prelucrările de date pe care le realizăm poate fi percepută până la urmă ca un lucru bun!

- Atunci când o persoană adresează o cerere de exercitare drepturi către operator, s-ar putea să formuleze și o plângere către **A.N.S.P.D.C.P**., iar pasul pe care îl face este pentru a putea justifica faptul că s-a adresat anterior operatorului (condiție impusă de Autoritate la depunerea plângerilor: *https://www.dataprotection.ro /index.jsp?page=Plangeri_pagina_principala*).

- Plângerile specifice protecției datelor pot fi depuse foarte simplu, online pe website-ul Autorității, mai sus menționat. În situația depunerii lor în condiții de legalitate, Autoritatea va demara o investigație asupra problematicii sesizate.

- Ar trebui să elaborați **o procedură internă de gestionare a plângerilor persoanelor vizate**. Aceasta poate fi identică sau foarte asemănătoare cu procedura de răspuns la cererile persoanelor vizate (**Anexa 6 Model de procedură de soluționare a cererilor persoanelor vizate**)

- Instruiți personalul cu privire la primirea plângerilor, respectiv la cum ar trebui să se adreseze pacientul (persoana vizată), în cazul în care dorește să depună o plângere.

- O plângere adresată împotriva medicului ori împotriva unității medicale în care își desfășoară activitatea, **poate avea consecințe deopotrivă asupra amândurora.**

- Oricărei plângeri ar trebui să i se ofere un răspuns complet în cel mai scurt timp, astfel încât să puteți menține sau chiar crește încrederea pacienților în unitatea medicală (operator).

Câteva detalii despre plângeri:

Chiar **dacă sunt adresate verbal**, ar trebui să ne notăm aspectele reclamate, să le investigăm și să le soluționăm. În acest mod putem dovedi bună credință, preocupare continuă și profesionalism.

Solicităm **mai multe detalii și clarificări** pentru orice aspect asupra căruia s-a depus plângerea. În acest fel dovedim o preocupare reală referitor la protecția datelor persoanelor care au adresat plângerea. Pentru aceasta ne putem întreba:

- Care sunt cauzele care au dus la adresarea plângerii?
- Ce s-a petrecut?
- Ce date cu caracter personal sunt puse în discuție?
- Au fost implicați angajați, colaboratori sau furnizori de servicii în producerea nemulțumirilor?

Orice **plângere ar trebui documentată**:

- Ce măsuri am luat? Spre exemplu, am luat măsuri disciplinare, am instituit noi politici sau proceduri pentru protejarea documentelor fizice (în cazul unei reclamații de acest tip)
- Ce avem în vedere pentru viitor? Ex: să schimbăm furnizorul de servicii care nu oferă garanții suficiente la nivel contractual (dacă vorbim despre reclamații cu privire la un soft folosit și nesecurizat de către dezvoltator)
- Cum tratăm efectele negative produse? (ex. recuperarea eventualelor sume de bani pentru recoltarea unor probe medicale prelevate dar compromise datorită unui furnizor de servicii de transport)
- Răspunsul oferit de noi ar trebui documentat astfel ca oricând să putem explica persoanei care justifică un interes real, respectiv autorităților, modalitatea de gestionare a cererii.

Atenție!

Dacă o plângere specifică protecției datelor a fost depusă către dumneavoastră, în calitate de medic, angajat al unei clinici sau al unui spital, **este foarte important să redirecționați această solicitare direct conducerii operatorului, ori Responsabilului cu Protecția Datelor.**

Cazuistică relevantă

Un pacient trimite o plângere prin e-mail către o clinică, în care afirmă că a primit materiale promoționale nesolicitate pe e-mail, deși nu și-a dat consimțământul pentru astfel de comunicări. Pacientul solicită să fie informat despre cum au fost obținute datele sale de contact și să fie șters din baza de date a clinicii pentru comunicări viitoare. Clinica nu are o procedură clară de gestionare a plângerilor și personalul nu este instruit în acest sens. În consecință, plângerea pacientului nu este tratată corespunzător și nu primește niciun răspuns în termenul de o lună prevăzut de lege. Această lipsă de răspuns poate duce la sancțiuni din partea autorităților de protecție a datelor și la pierderea încrederii pacienților în clinică.

Un medic este angajat/salariat la un cabinet medical individual care, în scop de organizare și marketing, utilizează un site propriu unde afișează fotografii și informații legate de angajații și colaboratorii săi, inclusiv chestiuni care țin de premii și realizări personale, cu sau fără legătură cu activitatea medicală. Acestuia nu i s-a comunicat la momentul angajării sale că datele din CV-ul prezentat la dosarul de recrutare vor fi expuse pe site-ul cabinetului. Observând la un moment dat aceasta, el sesizează angajatorul solicitându-i ca datele sale să fie șterse de pe site și să i se comunice măsurile de redresare. Angajatorul refuză acest lucru, motivând că este interesul legitim al său de a-ți face reclamă. O astfel de situație nu este conformă cu principiile protecției datelor, iar angajatorul ar putea fi sancționat de Autoritatea de Supraveghere.

Cazuistică din activitatea Autorității de Supraveghere:

Dent Estet Clinic SA - Autoritatea Națională de Supraveghere a finalizat în luna decembrie 2022 două investigații la un cabinet stomatologic și la un medic stomatolog, colaborator al cabinetului stomatologic, ambii operatori de date cu caracter personal. Investigațiile au fost demarate ca urmare a unei plângeri transmise de o persoană vizată prin care s-a reclamat faptul că operatorii Dent Estet Clinic SA și medicul colaborator i-au divulgat datele de sănătate în mediul online.

În cadrul investigațiilor efectuate, s-a constatat că operatorii au divulgat informații medicale referitoare la tratamentul ortodontic al petiționarului, constând într-un set de fotografii și radiografii care se puteau corela cu numele persoanei, prin publicarea unui articol pe un blog de specialitate. Aceste informații au fost publicate atât în scop științific, cât și în scop comercial.

S-a constatat că operatorul Dent Estet Clinic SA, deși a fost informat chiar de petiționar despre divulgarea neautorizată a datelor sale personale privind starea de sănătate, nu a notificat Autoritatea Națională de Supraveghere, în termen de cel mult 72 de ore de la data la care a luat la cunoștință de încălcarea de securitate, încălcând astfel art. 33 din Regulamentul (UE) 2016/679.

Sursă: https://www.dataprotection.ro/?page=Comunicat_Presa_31_01_2023_1

3.12 ORIENTĂRI CU PRIVIRE LA MODALITATEA DE RĂSPUNS ÎN CAZ DE ÎNCĂLCARE A SECURITĂȚII ȘI CONFIDENȚIALITĂȚII DATELOR PACIENTULUI SAU ALE ALTEI PERSOANE VIZATE

- Exemplificarea unor încălcări la adresa securității sau confidențialității datelor
- Identificarea pașilor de urmat în cazul în care s-a produs o încălcare la adresa securității sau confidențialității datelor

Regulamentul General privind Protecția Datelor (R.G.P.D.) caută **să protejeze persoanele vizate** (pe dumneavoastră sau pe diverse persoane fizice cu care dumneavoastră interacționați) prin stabilirea unor norme stricte privind prelucrarea datelor.

Articolele 32-34 din R.G.P.D. ne indică foarte clar măsurile recomandate dar și când trebuie să informăm A.N.S.P.D.C.P. sau persoanele vizate despre incidentele petrecute.

Incidentele de securitate *sunt acele situații în care datele cu caracter personal ar putea fi, datorită unui potențial ridicat de risc, sau sunt afectate, fie datorită unei acțiuni/inacțiuni umane, voluntare sau involuntare, fie datorită unui eveniment.*

Exemple de încălcări ale securității sau confidențialității datelor

- **Pierderea unui set de documente ale pacienților (ex:** fișe medicale**)**
- **Divulgarea informațiilor din foaia de observație către persoane neautorizate sau în spațiul public (ex:** La recepție pacientul este întrebat cu voce tare pentru ce analiză a venit, care este adresa sau codul PIN de la card, fără a asigura un cadru confidențial de discuție**)**
- **Fotografierea cu dispozitive personale a documentelor care conțin date medicale ale pacienților și transmiterea acestor documente către terți neautorizați**
- **Pierderea sau furtul unui dispozitiv portabil (telefon, laptop, tabletă) care conținea informații medicale despre pacient**
- **Predarea către firma care efectuează reparațiile dispozitivelor portabile (ex: laptop) sau vinderea dispozitivelor fără a șterge în condiții de siguranță datele medicale salvate pe acesta**
- **Transmiterea unor date medicale care vizează un pacient către un prieten medic sau către firme de dispozitive medicale / din domeniul farmaceutic / servicii de marketing și publicitate ș.a. fără ca acesta să fie autorizat în mod legal să aibă acces la date; transmiterea datelor către alți operatori, cum ar fi către firme de dispozitive medicale / farmaceutice / furnizori de alte servicii de marketing și publicitate, în absența consimțământului pacientului**

R.G.P.D. și legislația conexă fac distincție între diverse tipuri de încălcări și măsuri ce pot fi luate pentru a evita încălcările, însă ce trebuie reținut este că **operatorul trebuie să ia măsuri „rezonabile" în raport cu resursele de care dispune**, pentru a proteja datele. Astfel, nu este impus un standard de calitate în mod neapărat, ci **un regim de rigoare, prudență și diligență.**

Important de știut:

- **Este recomandat ca operatorul (spital, clinică, cabinet medical individual, alte forme de îngrijire medicală) să dețină o procedură sau un plan după care să acționeze în cazul în care s-a produs o încălcare.**

Exemplu: Un standard în domeniul gestionării securității informațiilor îl reprezintă standardul ISO 27001 care prevede o astfel de procedură de răspuns la incidentele de securitate a datelor (care pot fi și date cu caracter personal).

Ca medic, trebuie să știți că de îndată ce aflați despre un incident este foarte indicat să îl comunicați imediat Responsabilului cu Protecția Datelor sau conducerii operatorului pentru a lua măsurile imediate pentru remedierea situației.

Exemplu: Ați pierdut laptopul de serviciu fiind într-o deplasare. Pe acesta se aflau buletine de analize medicale ale câtorva sute de pacienți.

Cooperați cu colegii juriști, informaticieni sau persoane cu atribuții în domeniul protecției datelor. Au nevoie de ajutorul dumneavoastră imediat pentru a remedia neîntârziat o problemă!

Exemplu: O persoană fotografiază un pacient minor abandonat în spital după naștere. Fiind sensibilizată de aceasta, organizează pe cont propriu o campanie online (pe Facebook) de adoptare a persoanei. O astfel de speță poate ridica deosebit de multe probleme minorului atât în prezent cât și în viitor. În cazul de față, echipa medicală care a avut acces la minor poate ajuta responsabilul cu protecția datelor ori managementul unității (care poate fi cabinet medical individual) să identifice cu exactitate traseul fotografiei și circumstanțele concrete care au permis realizarea fotografiei: situația poate fi un incident, dacă nu există nici un consimțământ și nici măcar vreo informare însă, aceeași situație ar putea să nu fie incident dacă în vreun fel a existat un interes superior al copilului de a se demara respectiva campanie și un reprezentant al autorității care a încuviințat chiar și verbal realizarea fotografiei și demararea campaniei publicitare.

Atunci când operatorul constată o breșă de securitate (un incident major) se impune notificarea către A.N.S.P.D.C.P. în termen de 72 ore de la descoperirea incidentului, accesând formularul următor: *https://www.dataprotection.ro/formulare/formularBresaGdpr.do?action=view_action&newFormular=true*

Anumite incidente pot implica chiar și informarea organelor de urmărire penală întrucât poate fi vorba de furt, infracțiuni de fals sau infracțiuni informatice!

Exemplu: Un cadru medical sustrage din arhivă un set de documente care nu îl privesc, fiind de gardă pe durata nopții. Realizează o copie a lor (le fotografiază), le transmite unei persoane interesate și le depune înapoi în arhivă ulterior transmiterii.

Raportarea incidentelor de securitate

Raportarea incidentelor poate fi obligația operatorului de date, astfel dumneavoastră în calitate de medic trebuie să cunoașteți că de îndată ce este determinată natura încălcării, amploarea acesteia și potențialele prejudicii, trebuie să se raporteze prin Responsabilul cu Protecția Datelor sau unde nu există, în mod direct de către medicul care are atribuțiile de administrare ale unității de îngrijire medicală (cum este cazul cabinetelor medicale individuale sau a formelor de asociere, cum este cazul societăților cu răspundere limitată - SRL):

- Tipul de date afectate (ex: datele consemnate în CI)
- Tipul de documente (ex: contract, fișa clientului)
- Dacă sunt afectate date sensibile (ex: date medicale)
- Dacă există mecanisme de securitate sau protecție a datelor afectate (ex: parole)
- Dacă datele au fost sau nu divulgate unei terțe părți (ex: datele au fost publicate pe o rețea de socializare)
- Dacă datele în cauză ar putea să prejudicieze iremediabil o persoană (ex: dezvăluirea unor afecțiuni medicale)
- Numărul de persoane afectate
- Măsurile tehnice și organizatorice luate anterior, în timpul și ulterior petrecerii evenimentului

Între anexele puse la dispoziție, puteți găsi și un model de **Plan de reacție la incidentele specifice protecției datelor cu caracter personal** (*Anexa 8 - Procedură privind managementul incidentelor de securitate*).

Raportarea incidentelor (așa zisa auto denunțare) **poate atrage sancțiuni**! Totuși, **nu toate incidentele trebuie raportate** – așa cum puteți vedea din diagrama prezentată la sfârșitul acestui capitol.

Lipsa raportării însă, atunci când aceasta era necesară, va atrage cu siguranță sancțiuni mult mai mari dacă incidentele sunt raportate de altcineva decât operatorul sau chiar de către o persoană afectată!

Cazuistică relevantă

Un spital deține informații confidențiale despre pacienții săi, precum date de identificare, istoric medical, rezultate ale analizelor și alte informații sensibile. Un angajat al spitalului primește un e-mail aparent legitim prin care îi cere să descarce un atașament important. Fără să știe, angajatul descarcă un program malware, care criptează toate fișierele de pe sistemul informatic al spitalului și blochează accesul la acestea.

Spitalul nu are un plan de reacție la incidente și nu știe cum să gestioneze situația. Ca urmare, accesul la informațiile medicale ale pacienților este blocat pentru o perioadă îndelungată, ceea ce împiedică furnizarea unor servicii medicale adecvate și în timp util. În plus, spitalul nu știe cum să comunice incidentul către autoritățile competente sau către pacienții afectați, ceea ce crește riscul de sancțiuni și afectează încrederea pacienților în instituție.

În concluzie, medicul sau medicii care se confruntă cu o situație în care constată că sistemul informatic sau un sistem electronic nu mai este disponibil, nu trebuie să aștepte ca acesta să își revină de la sine, ci trebuie imediat să anunțe fie responsabilul cu protecția datelor, fie o persoană cu atribuții de administrare din cadrul unității medicale.

Cazuistică din activitatea Autorității de Supraveghere:

Actamedica SRL din Târgu-Mureș a transmis o informare unei persoane fizice în legătură cu pierderea probelor sale biologice și a unei sume de bani trimise prin intermediul unei firme de curierat, coletul ajungând deteriorat la destinatar. La solicitarea de a i se comunica ce date personale i-au fost expuse cu această ocazie și dacă A.N.S.P.D.C.P. a fost notificată în legătură cu acest incident, în răspunsul trimis operatorul a indicat persoanei fizice datele de contact ale avocatului societății și o adresă de e-mail de la firma de curierat către care să își exprime ”doleanțele”. Nu a notificat incidentul. Amenda pentru incident a fost de 2000 € și pentru lipsa notificării 1000 €.

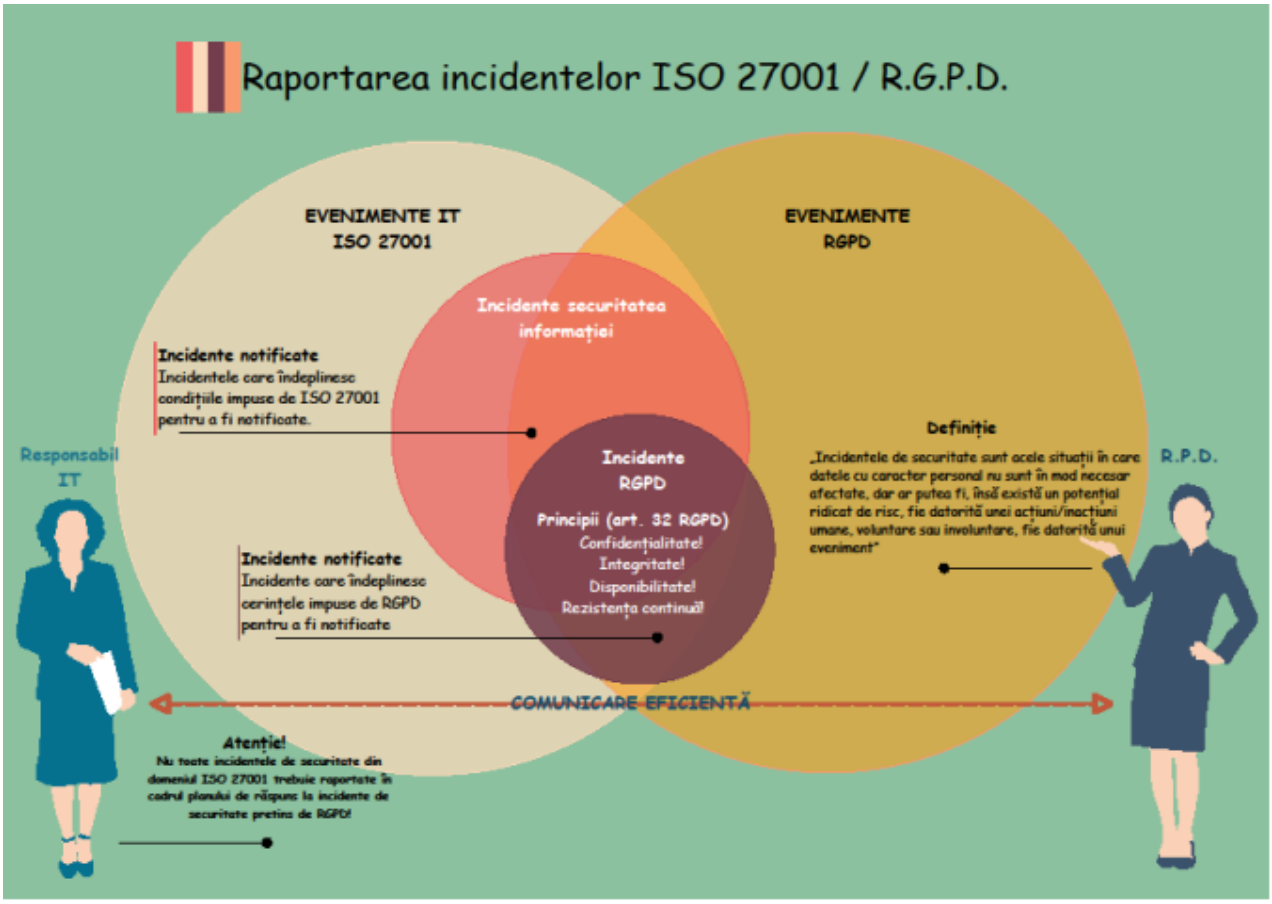
(https://www.dataprotection.ro/?page=Comunicat_Presa_24_08_2021&lang=ro)

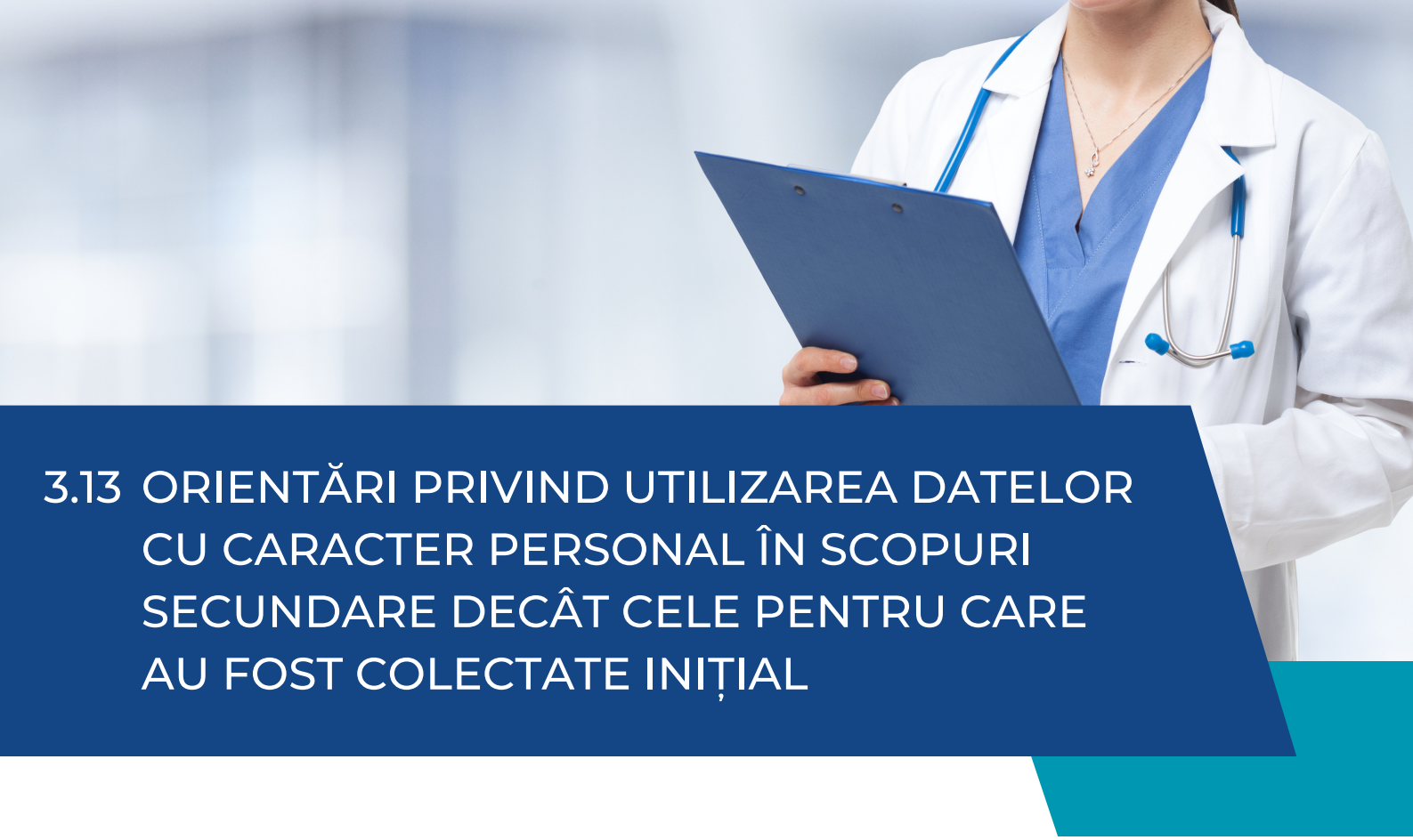
Scurtă reprezentare a cazurilor de raportare a incidentelor:

În imaginea de mai jos se evidențiază două categorii de situații care trebuie cunoscute, ambele situații specifice pot sau nu să se suprapună, ambele pot sau nu constitui incidente și în situația ambelor poate fi necesară raportarea incidentului către o autoritate publică.

O categorie de situații sunt cele avute în vedere de standardul ISO 27001, standard care impune măsuri pentru a se asigura securitatea și siguranța sistemelor informatice, în special împotriva fraudării acestora, afectându-li-se capacitățile de funcționalitate și securitatea datelor. Spre exemplu, dacă a fost generat un virus malware, incidentul ar trebui notat și raportat la autoritatea publică națională cu atribuții în domeniul securității cibernetice. Pe linie specifică acestor categorii de incidente de securitate sunt cei care lucrează în calitate de experți informaticieni în cadrul unei unități medicale.

Însă, aceeași situație de mai sus poate pune în pericol și date cu caracter personal, caz în care problematica devine una mai complexă, deoarece nu mai este vorba, exclusiv, de securitatea și siguranța unui sistem informatic ci, în plus, mai este vorba de riscul asupra datelor personale ale unor persoane fizice și impactul asupra dreptului acestora la confidențialitate și la protecția datelor cu caracter personal. Când există un asemenea risc și el nu poate fi îndepărtat (tratat!), problematica este una specifică de protecția datelor personale și trebuie sesizată responsabilului cu protecția datelor și mai departe să parcurgă un lanț de măsuri tipice reacției la un incident de securitate. Aceasta ar fi a doua mare categorie de situații de incidente care trebuie raportate, potrivit Regulamentului General privind Protecția Datelor.





3.13 ORIENTĂRI PRIVIND UTILIZAREA DATELOR CU CARACTER PERSONAL ÎN SCOPURI SECUNDARE DECÂT CELE PENTRU CARE AU FOST COLECTATE INIȚIAL

- Prezentarea cazurilor în care sunt permise prelucrările secundare ale datelor

- Prezentarea situațiilor în care nu se pot folosi datele în scop secundar, fără un alt temei legal valid (ex. un consimțământ)

Ca regulă generală, Regulamentul General privind protecția datelor **permite prelucrarea datelor în scopuri secundare**, cum este cel al cercetării științifice, medicale, istorice sau în scopuri statistice. Prevederile legale explicite sunt: art. 6 alin. (4), art. 9 alin. (2) lit. h), art. 9 alin. (3), art. 89.

Aspectele principale de care trebuie ținut cont sunt următoarele: urmărirea ca scopurile să fie compatibile cu scopul inițial al colectării datelor și, atunci când este posibil, luarea de măsuri prin care să nu se mai permită identificarea persoanelor vizate (Ex. pseudonimizarea sau anonimizarea datelor).

Ce ar trebui să cunoașteți:

Identificarea persoanelor este posibilă atât prin observarea unor date care pot duce **direct la identificare** (ex. un cod unic, precum C.N.P.-ul) cât și prin **coroborarea mai multor seturi de informații** care pot duce **indirect la identificarea** persoanei (ex. coroborarea diagnosticului cu vârsta, cu sexul, cu tratamentul oferit și cu locația unde s-a oferit tratamentul).

O simplă măsură de pseudonimizare a datelor nu este întotdeauna suficientă pentru a împiedica identificarea unei persoane.

- **Exemplu**: Cercetând cazuistica privind condamnările penale de pe portalurile online dedicate acestui subiect veți putea corobora mai multe informații care, împreună cu inițialele persoanelor implicate într-un proces, vă asigură identificarea persoanelor (ex. A.N. a comis o infracțiune de luare de mită într-un proces cu Ministerul X, aspect din care ne putem da seama că A.N. pot reprezenta inițialele unei persoane publice, ex. Adrian Năstase). Astfel acest lucru dovedește că, în anumite cazuri, simpla pseudonimizare nu este suficientă.

Puteți folosi un **sistem propriu de protejare a identității persoanelor** atunci când doriți să folosiți datele în scopuri secundare precum cel al studiilor clinice. O recomandare ar putea fi alocarea unui număr pacientului.

- **Exemplu**: Pentru pregătirea unei prezentări în cadrul unui congres veți căuta să eliminați din imagistica folosită elemente care, coroborate, pot identifica persoana. În schimb puteți aloca un număr – pacientul nr. 675. Însă trebuie să vă asigurați că documentul intern în care ați făcut coroborarea este securizat și păstrat în condiții ridicate de confidențialitate.

Prelucrarea datelor în scopuri statistice este întru totul compatibilă cu prevederile R.G.P.D.

- **Exemplu**: Un grup de medici de la un spital decide să efectueze un studiu epidemiologic pentru a urmări răspândirea unei anumite boli în comunitate. Pentru a face acest lucru, ei colectează date de la pacienții lor, inclusiv vârstă, sex, locație geografică, istoric medical și alte informații relevante pentru boala studiată. Înainte de a începe analiza datelor, medicii se asigură că toate datele sunt fie anonimizate (adică orice informație care ar putea identifica o persoană este eliminată), fie pseudonimizate (adică identificatorii direcți sunt înlocuiți cu pseudonime). Acest proces asigură că persoanele nu pot fi identificate din datele colectate, protejând astfel confidențialitatea pacienților.

Pentru cazuri speciale ori deosebit de grave care se doresc a fi mediatizate se impune colectarea consimțământului persoanei vizate ori a reprezentantului legal al acestuia. Alăturat, în **Partea a IV-a**, găsiți un model de declarație de consimțământ: **Anexa 4 Consimțământ specific R.G.P.D.**

- **Exemplu**: vedem adesea campanii de strângere de fonduri pentru diverse persoane cu boli rare ori dizabilități. Pentru ca să existe o acoperire legală pentru această acțiune se impune ca în prealabil să fie obținut consimțământul persoanei și acesta să fie valid conform legii.

Cazuistică relevantă

Unitatea medicală XYZ, în dorința de a promova serviciile și tratamentele inovatoare pe care le oferă, a decis să realizeze un studiu privind eficacitatea unui tratament nou pentru o afecțiune specifică. Fără a obține consimțământul pacienților și fără să se asigure de anonimizarea datelor, unitatea a prelucrat și analizat informațiile medicale ale pacienților care au beneficiat de tratament.

Ulterior, pentru a crește vizibilitatea studiului, unitatea medicală a publicat rezultatele pe site-ul său și pe rețelele de socializare. Datele pacienților, inclusiv informații privind diagnosticul, vârsta și tratamentul au fost expuse, permițând astfel identificarea indirectă a persoanelor vizate.

Un jurnalist a sesizat publicarea acestor informații și a scris un articol de investigație care a evidențiat încălcarea confidențialității pacienților și lipsa consimțământului acestora. În urma acestui incident, unitatea medicală a fost supusă unor investigații din partea autorităților de reglementare, a fost sancționată cu amenzi semnificative și a pierdut încrederea pacienților și a comunității medicale.

Acest incident ar fi putut fi evitat dacă unitatea medicală ar fi obținut consimțământul pacienților pentru prelucrarea datelor în scopuri secundare și ar fi implementat măsuri de protecție adecvate pentru a asigura confidențialitatea datelor.

Cazuistică din activitatea Autorității de Supraveghere:

Autoritatea de supraveghere din Italia (Garante) a aplicat o amendă de 5000 euro unui medic întrucât s-a demonstrat că radiografii / diapozitive ale unui caz clinic în care fusese implicat medicul au fost prezentate la un congres și ulterior acestea au fost publicate pe website-ul Società triveneta di chirurgia.

Slide-urile prezentării publicate conțineau date personale ale unui pacient, cum ar fi inițialele pacientului, vârsta, sexul, istoricul medical detaliat al pacientului, detaliile internărilor din 1980 până în 2016 și procedurile chirurgicale efectuate în perioada respectivă, data internării, secția de chirurgie care a efectuat procedurile, zilele petrecute în spital, numeroase imagini de diagnostic și 22 de fotografii care arată pacientul în timpul operațiilor.

Nu s-a putut dovedi că persoana vizată și-ar fi dat consimțământul pentru aceste prelucrări de date.

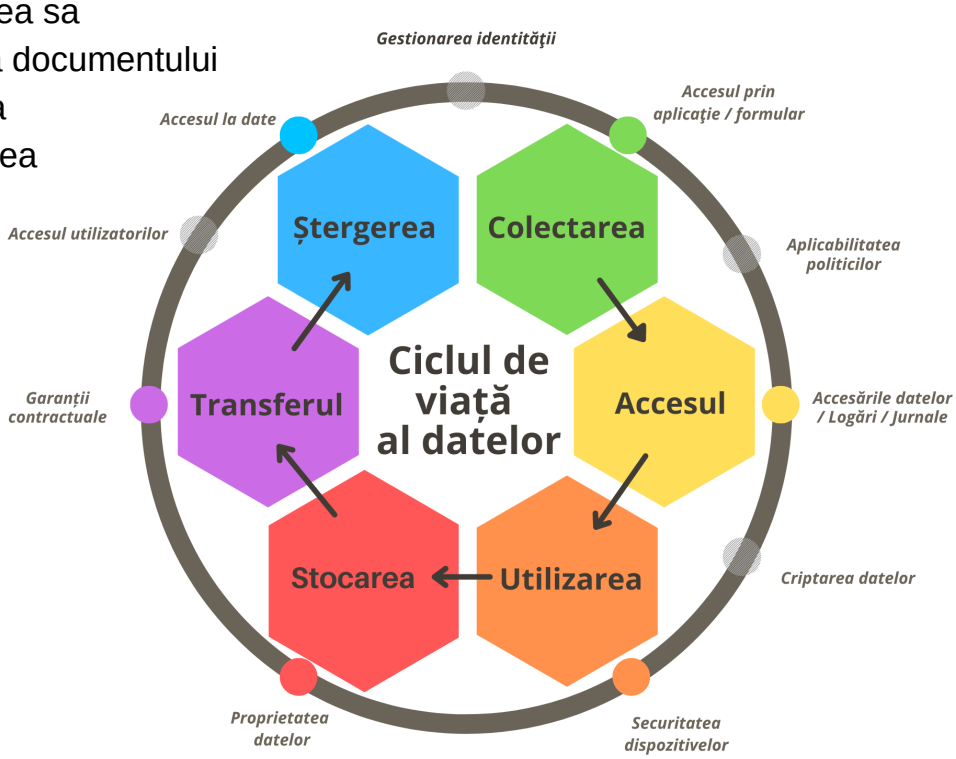
Sursa: *Ordinanza ingiunzione - 15 aprile 2021 - Garante Privacy*

3.14 ORIENTĂRI PRIVIND DISTRUGEREA ÎN SIGURANȚĂ A DATELOR CU CARACTER PERSONAL

Explorarea celor mai bune practici pentru distrugerea în siguranță a documentelor care conțin date cu caracter personal, atât prin metode interne, cât și prin externalizarea serviciilor

Orice document (fizic sau electronic) care conține date cu caracter personal are un **„ciclu de viață”**. Astfel, vorbim despre:

- Crearea documentului
- Analiza / folosirea acestuia
- Distribuirea sa
- Utilizarea documentului
- Arhivarea
- Distrugerea



Pentru a ne asigura că respectăm întru totul normele privind protejarea vieții private și a datelor cu caracter personal este foarte indicat să acordăm o atenție sporită documentelor aflate în **ultimele faze ale ciclului de viață – arhivarea și mai ales distrugerea** acestora. În continuare vom dezvolta câteva practici în acest sens.

Prezenta Orientare se adresează operatorilor de date (unităților medicale, furnizorilor de servicii medicale, indiferent că sunt constituiți într-o entitate cu sau fără personalitate juridică). Medicii, în special cei cu atribuții de management sau de reprezentare a operatorului, vor avea în vedere această perspectivă, deoarece sunt parte a sistemului de resurse umane din cadrul operatorului.

Ce ar trebui să cunoașteți:

Orice informații vehiculăm pe suport de hârtie sau în format electronic se încadrează într-o categorie de date, care trebuie regăsite într-un nomenclator al operatorului, unde se menționează perioada de deținere a documentului și alte informații. Odată ce această perioadă este îndeplinită, se trece la operațiunea de distrugere a suportului de informație, operațiune la care se referă prezenta Orientare.

Distrugerea documentelor se poate realiza atât **direct** de dumneavoastră în cadrul unității medicale sau, atunci când este vorba de un volum mare de documente care trebuie distruse, se poate alege un **furnizor de servicii de distrugere** a acestora. Haideți să vedem ce trebuie însă să avem în vedere:

Metode interne de distrugere a datelor

- **Tocătoare de documente**: Utilizarea unor tocătoare de documente este o metodă eficientă pentru distrugerea în siguranță a documentelor în format fizic. Alegeți tocătoare care să taie documentele în fâșii înguste sau particule mici, pentru a face dificilă, dacă nu imposibilă, reconstituirea informațiilor.
    - **Exemplu**: Simpla aruncare la coșul de gunoi a unor documente expune unitatea medicală sau chiar pe dumneavoastră (în cazul nerespectării procedurilor și politicilor interne). În secțiunea cazuistică vom dezvolta o astfel de speță.

- **Demagnetizarea**: Pentru distrugerea datelor stocate pe suporturi magnetice (ex. CD-uri, hard disk-uri, benzi magnetice) demagnetizarea este o soluție eficientă.

Aceasta constă în utilizarea unui aparat de demagnetizare (degausser) pentru a distruge informațiile prin expunerea suportului la un câmp magnetic puternic.

- **Exemplu**: Pierderea unui CD (nesecurizat) care conține rezultatele unor analize medicale ale unui pacient poate constitui un incident care să atragă sancțiuni mari!

- **Ștergerea securizată a datelor**: În cazul dispozitivelor de stocare electronică (ex. hard disk-uri, memorii flash) utilizați un software de ștergere securizată pentru a distruge ori suprascrie datele de mai multe ori, astfel încât să nu poată fi recuperate.
  - **Exemple**: CCleaner, Eraser, BitRaser sunt câteva exemple de astfel de softuri. Puteți alege orice soft identificați ca fiind facil pentru această activitate. Atenție! Vă rugăm să vă asigurați că furnizorul de soft respectă normele R.G.P.D. (adesea acest angajament este luat prin politica de confidențialitate publicată pe website sau informații relevante se pot găsi în termeni și condiții).

Servicii externalizate de distrugere a datelor

- **Evaluarea furnizorilor**: Dacă alegeți să externalizați procesul de distrugere a datelor, asigurați-vă că furnizorul ales respectă standardele R.G.P.D. și oferă garanții adecvate în ceea ce privește securitatea și confidențialitatea datelor. Cereți recomandări de la alți colegi care colaborează cu furnizori exemplari!
  - **Exemplu**: Așa cum menționam și mai sus, studiați angajamentele pe care aceștia și le iau pentru a respecta normele legale (detaliate în politica de confidențialitate sau termeni și condiții). Dacă nu își asumă nici un fel de răspundere pentru distrugerea securizată și în condiții de confidențialitate, dar să poată să și demonstreze acest lucru, evitați furnizorul de servicii respectiv!

- **Acorduri privind protecția datelor**: Încheiați un acord de confidențialitate și protecție a datelor cu furnizorul, care să detalieze responsabilitățile și obligațiile acestuia în legătură cu procesul de distrugere a datelor.
  - **Exemplu**: Cel mai adesea un furnizor responsabil va pune la dispoziția dumneavoastră un acord specific (operator-persoană împuternicită) pentru distrugerea acestor date.

- Urmăriți atent procesul detaliat pentru distrugere și felul în care acesta este documentat! În cazul în care nu vă este transmis un astfel de acord, solicitați unul ori folosiți unul generic pus la dispoziție în acest ghid (**Anexa 2 Model de acord de confidențialitate pe care să îl utilizați în relație cu colaboratorii persoane împuternicite**)

- **Monitorizarea activității furnizorului**: Solicitați rapoarte și documentație referitoare la procesele de distrugere și verificați ca procesele să fie duse la îndeplinire cu succes.
  - **Exemplu**: puteți solicita furnizorului filmări cu procesul de distrugere a documentelor.

- **Documente doveditoare ale distrugerii**: După ce datele au fost distruse în mod corespunzător, furnizorul ar trebui să vă ofere un document care să ateste eliminarea completă și sigură a datelor. Acest document poate fi folosit ca dovadă în cazul unor audituri sau controale privind protecția datelor.
  - **Exemplu**: Un astfel de document poate fi un raport, un proces verbal de distrugere, un certificat sau un alt document de asumare a acestei răspunderi a furnizorului.

Recomandări suplimentare

- **Politici și proceduri interne**: Elaborați politici și proceduri interne care să reglementeze modul în care datele cu caracter personal sunt distruse în cadrul cabinetului medical sau al unității medicale în care vă desfășurați activitatea. Asigurați-vă că aceste politici sunt respectate de întregul personal și că toți angajații sunt instruiți în legătură cu responsabilitățile lor privind protecția datelor.
  - **Exemplu**: Poate fi vorba despre o procedură operațională de distrugere a documentelor prin care se va constitui o comisie de distrugere a documentelor, care pe baza unui inventar al documentelor ce vor fi distruse, le vor distruge și vor documenta aceasta printr-un proces verbal de distrugere semnat de toți membrii comisiei.

- **Revizuirea periodică a datelor**: Stabiliți un program de revizuire periodică a datelor stocate pe documente pentru a identifica informațiile care nu mai sunt necesare și care trebuie distruse în mod corespunzător.
  - **Exemplu**: Unele documente trebuie păstrate pe o perioadă lungă de timp, fiind o obligație legală a unității medicale conform legislației în vigoare (Legea 16/1996 privind Arhivele Naționale), în timp ce pentru altele nu identificați un termen stabilit de lege.

În acest caz stabiliți intern un termen rezonabil pentru păstrarea datelor raportându-ne la scopul colectării datelor.

- **Consultarea responsabilului cu protecția datelor**: Dacă este cazul, adresați-vă responsabilului cu protecția datelor (DPO) din cadrul unității medicale, care să vă coordoneze procesul de distrugere a datelor cu caracter personal. În situația unor operatori de date cu personal medical extrem de restrâns, fără a avea angajat un DPO, cum ar fi unele cabinete medicale individuale sau SRL-uri, acestea pot fie singure să-și stabilească clar procedura, fie să apeleze la un consultant.

Cazuistică relevantă

Clinica Medicală "Sănătate Plus" este o unitate medicală privată care oferă o gamă largă de servicii medicale, de la consultări și analize de laborator până la intervenții chirurgicale. Într-o zi, sistemul informatic al clinicii a fost atacat de hackeri, care au reușit să acceseze și să sustragă date cu caracter personal ale pacienților, inclusiv nume, adrese, numere de telefon, istoric medical și detalii despre tratamentele prescrise.

Ca urmare a acestui incident, conducerea clinicii a luat măsuri pentru a îmbunătăți securitatea informațiilor stocate în sistemul lor. Aceste măsuri au inclus actualizarea software-ului de securitate, implementarea unor metode mai avansate de criptare a datelor și instruirea personalului cu privire la importanța protejării datelor cu caracter personal.

De asemenea, clinica a informat pacienții afectați despre incident și le-a oferit asistență pentru a le proteja identitatea și a preveni posibilele fraude.

Cu toate acestea, în pofida măsurilor luate, datele compromise au fost deja expuse și pot fi utilizate în moduri ilicite de către terțe părți. Autoritatea națională de protecție a datelor a deschis o investigație privind incidentul și, în urma constatărilor, a decis să sancționeze Clinica "Sănătate Plus" cu o amendă semnificativă pentru nerespectarea prevederilor legale privind protecția datelor cu caracter personal.

Cazuistică din activitatea Autorității de Supraveghere:

Medlife S.A. – amendă aplicată de A.N.S.P.D.C.P. 5000 euro

O persoană fizică a identificat documente care conțineau date cu caracter personal, inclusiv date sensibile, la coșul de gunoi al unei unități administrativ teritoriale. Documentele conțineau date ale pacienților Medlife S.A. În cadrul investigației s-a constatat că operatorul nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de confidențialitate și securitate corespunzător riscului prezentat de prelucrare, ceea ce a condus la accesarea ori divulgarea ilicită a datelor cu caracter personal ale clienților proprii MEDLIFE S.A. (nume, prenume, CNP, serviciul medical de care a beneficiat, analiza medicală efectuată, suma achitată, cont bancar) și ale angajaților săi (salariu avans) în perioada iulie 2020 – august 2020.

Sursa: *https://www.dataprotection.ro/?page=Comunicat_Presa_24_05_2022*

Cazuistică internațională:

British Pregnancy Advisory Service (BPAS) este o organizație caritabilă din Marea Britanie care oferă consiliere și servicii conexe procedurilor de avort. În anul 2012, BPAS a fost victima unui atac cibernetic, care a dus la accesarea ilegală a peste 9.000 de fișiere care conțineau informații personale și medicale despre pacienți. Informațiile furate includeau numele, adresa, data de naștere, numărul de telefon și istoricul medical al pacienților, precum și informații despre avorturile pe care le-au avut sau intenționau să le facă. Autoritățile au stabilit că BPAS nu a luat măsurile adecvate pentru a proteja aceste informații și pentru a preveni un astfel de atac.

Ca urmare, BPAS a fost amendată cu 200.000 de lire sterline de către Information Commissioner's Office (I.C.O.) autoritatea de supraveghere a protecției datelor din Marea Britanie, în noiembrie 2014.

Sursa: *https://www.thirdsector.co.uk/british-pregnancy-advisory-service-fined-200000-hacker-accessed-information/communications/article/1284156*

3.15 ORIENTĂRI PRIVIND PROTEJAREA DATELOR ATUNCI CÂND UN MEDIC ÎȘI ÎNCETEAZĂ ACTIVITATEA

Prezentarea unor bune practici și a unor rele practici pe care le întâlnim atunci când un medic își încetează activitatea în cadrul unei unități medicale (spital, clinică, cabinet individual)

Când un medic își încetează activitatea în cadrul unei unități medicale, chiar și la acel moment și ulterior, este esențial să respecte principiile R.G.P.D. pentru a proteja datele pacienților și a evita sancțiuni.

Ce ar trebui să cunoașteți în materie de Bune practici:

Respectarea dreptului la confidențialitate: Un medic trebuie să se asigure că informațiile pacienților rămân confidențiale și protejate, **chiar și după încetarea activității sale**. Acest lucru implică respectarea politicii interne de securitate a unității medicale și a legislației aplicabile.

- **Exemplu**: Nu este îngăduit medicului să ofere informații unor terțe persoane (ex. agenții de presă) despre un pacient, spre exemplu pentru că este o persoană publică, care a urmat un tratament sub îndrumarea acestuia, dar care acum este implicat într-un scandal mediatic.

Transferul responsabilității: Înainte de a părăsi unitatea medicală, medicul trebuie să transfere responsabilitatea datelor personale ale pacienților săi către un alt medic sau către o persoană desemnată responsabilă. Procesul trebuie să fie bine documentat și să includă notificarea pacienților cu privire la acest transfer.

- **Exemplu**: predarea dispozitivelor mobile (laptop, telefoane, tablete ș.a.) pe care sunt stocate date cu caracter personal se face printr-un proces verbal de predare-primire către personalul cu atribuții specifice din cadrul operatorului (unității medicale). Operatorul de date va putea pune la dispoziția altei persoane aceste dispozitive.

Asigurarea securității datelor: Medicul trebuie să se asigure că toate informațiile sensibile ale pacienților sunt depozitate într-un mediu securizat și accesibile doar de către persoanele autorizate. Orice fel de chei de acces (fizice sau digitale) vor fi predate doar personalului autorizat de către unitatea medicală.

- **Exemplu**: nu vom lăsa la dispoziția registratorilor medicali, asistenților medicali sau personalului care nu ar putea avea atribuții specifice de a avea acces la buletinele analizelor medicale ale pacientului. Dimpotrivă, acestea se pot depozita într-un dulap metalic, închis cu cheie, care va fi predată la încetarea activității personalului cu atribuții specifice în acest sens (ex. personalului de resurse umane, superiorului ierarhic sau persoanei desemnate de unitatea medicală).

Eliminarea corectă a datelor: În cazul în care un medic deține copii ale datelor pacienților în format fizic sau electronic, acestea trebuie să fie eliminate în mod corespunzător și în conformitate cu regulile GDPR. Acest lucru implică utilizarea unor metode de ștergere sigure, care previn recuperarea datelor.

- **Exemplu**: înainte de încetarea relațiilor de muncă, orice fel de copii ale documentelor / analizelor avute, care nu mai servesc vreunui scop și pentru care nu există un termen legal de păstrare sau nu este cazul a fi predate către operator, să fie distruse (prin tocător sau alte mecanisme specifice).

Ce ar trebui să cunoașteți în materie de Rele practici:

Păstrarea datelor fără autorizare expresă: Un medic nu trebuie să păstreze informații despre pacienți în format fizic sau electronic după încetarea activității sale în cadrul unității medicale, fără un motiv legitim și o autorizare expresă din partea operatorului.

- **Exemplu**: Este interzisă prelucrarea datelor pacienților ulterior încheierii relației contractuale cu operatorul – unitate medicală, dacă nu există o prevedere legală sau vreo solicitare expresă a operatorului în acest sens.

Divulgarea neautorizată a datelor: Orice distribuire a informațiilor pacienților către terțe părți, fără consimțământul acestora sau fără a fi în conformitate cu legile în vigoare, reprezintă o încălcare a GDPR.

- **Exemplu**: Răzbunarea pe operator prin publicarea pe Facebook a anumitor date ale pacienților, pentru o decizie de concediere, poate atrage sancțiuni directe asupra medicului (persoanei fizice) care a divulgat datele!

Lipsa unui plan de tranziție clar: Înainte de a părăsi unitatea medicală, operatorul trebuie să dețină un plan de tranziție pentru a se asigura că pacienții vor continua să beneficieze de îngrijiri medicale adecvate și că datele lor vor fi gestionate în mod corespunzător. Lipsa unui astfel de plan poate duce la întreruperea relațiilor dintre pacient și operator (unitate medicală), o decredibilizare a acestuia sau o lipsă de încredere în noul medic care va prelua pacienții. Totodată, pot apărea provocări specifice protecției datelor cu caracter personal cum ar fi: *medicului nou să nu îi fie puse la dispoziție toate analizele medicale efectuate, rezultatele dar și alte documente relevante, în lipsa cărora să nu poată oferi indicații clare pacientului!*

Accesul neautorizat la sistemele informatice ale unității medicale: După ce un medic își încetează activitatea în cadrul unității medicale, trebuie să i se revoce orice acces la sistemele informatice ale unității și la documentele conținând datele pacienților. Permiterea accesului neautorizat la aceste sisteme poate duce la abuzuri și încălcări ale drepturilor pacienților.

- **Exemplu**: Adresa de e-mail de serviciu trebuie preluată de o altă persoană sau trebuie inactivată odată cu întreruperea relațiilor de muncă sau prestări servicii cu caracter medical. Continuarea vizualizării corespondenței în afara relației contractuale expune ambii, atât medicul cât și unitatea medicală, la riscuri specifice protecției datelor cu caracter personal.

În concluzie, protejarea datelor pacienților este o responsabilitate esențială a medicilor, chiar și după ce își încetează activitatea în cadrul unei unități medicale. Respectarea principiilor GDPR și evitarea practicilor nesigure poate ajuta la asigurarea securității și confidențialității datelor personale ale pacienților, reducând riscul de sancțiuni și protejând reputația unității medicale.

Cazuistică relevantă

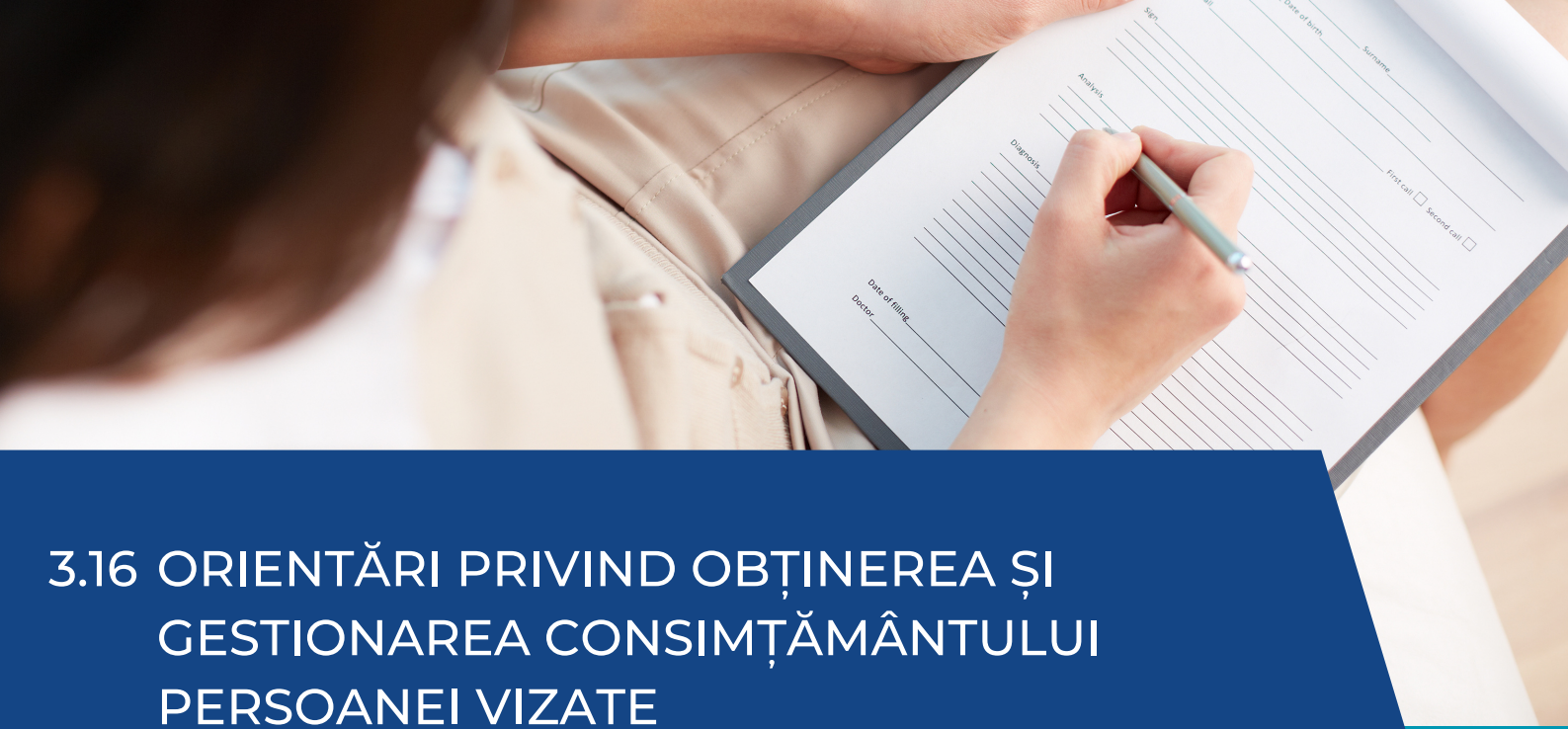
Într-un caz ipotetic, un medic a decis să își înceteze activitatea în cadrul unei unități medicale private, dar nu a informat în mod corespunzător pacienții săi despre această schimbare. În timp ce clinica a desemnat un alt medic pentru a prelua cazurile pacienților, lipsa comunicării adecvate a lăsat pacienții confuzi și neliniștiți, neștiind cui să i se adreseze pentru a obține informații despre tratamentul lor în curs sau despre următorii pași în îngrijirea medicală.

Această neglijare în comunicarea cu pacienții ar putea fi considerată o practică nesigură, deoarece poate duce la perturbarea continuității îngrijirii medicale și poate afecta încrederea pacienților în unitatea medicală și în personalul său. De asemenea, aceasta poate avea implicații negative asupra protecției datelor cu caracter personal, în cazul în care pacienții decid să-și transfere dosarul medical la o altă unitate medicală, fără ca această tranziție să fie gestionată corespunzător de către unitatea medicală inițială.

Cazuistică internațională:

Centrul medical **London Surgery Bayswater Medical Care** (BMC) a fost amendat de către Autoritatea de Supraveghere (Information Commissioner's Office – I.C.O.) din Marea Britanie cu 35000 GBP (aproximativ 40000 euro), pentru lipsa asigurării securității și confidențialității datelor pacienților. În speță, este vorba despre faptul că unitatea medicală și-a mutat activitatea la o nouă locație, păstrând însă vechea locație ca spațiu de stocare a documentelor pacienților. Din investigație a reieșit că un număr mare de documente medicale erau abandonate și puteau fi vizualizate prin geamul clădirii, securizarea constând într-un singur lacăt.

Sursa: *https://www.itgovernance.co.uk/blog/gp-practice-fined-35k-for-failing-to-secure-medical-records*



3.16 ORIENTĂRI PRIVIND OBȚINEREA ȘI GESTIONAREA CONSIMȚĂMÂNTULUI PERSOANEI VIZATE

Un plus de claritate cu privire la situațiile în care se va obține consimțământul specific R.G.P.D. al persoanei vizate (pacient, medic)

În capitolele anterioare a fost prezentată pe larg situația obținerii consimțământului persoanei vizate (a pacientului, de regulă) în diversele sale ipostaze de interacțiune cu unitatea medicală ca operator de date sau cu medicul în calitate de angajat, respectiv colaborator al acesteia. Concluziile au fost în principal două:

- Se impune o diferențiere clară a necesității:
  - **Notei de informare a persoanei vizate cu privire la prelucrările de date** - cu scopul de a-l informa la modul general despre toate prelucrările de date care se realizează în toate interacțiunile dintre pacient și unitatea medicală
  - Formularului numit **„Acordul pacientului informat” -** scopul principal al acestuia fiind acceptarea urmărilor actului medical la care este supus
  - **Consimțământului specific R.G.P.D**.- care are ca scop și utilitate strict situațiile în care se dorește o prelucrare de date afară de tot ceea ce prevede legea în mod expres, cum ar fi prelucrări legate de marketing, promovare, publicitate sau cercetare științifică.

- Există loc de îmbunătățire a cadrului legislativ

Ce ar trebui să cunoașteți în materie de Bune practici:

Utilizați un **consimțământ specific R.G.P.D.** de fiecare dată când doriți să folosiți informațiile personale ale pacientului **în scop de promovare, publicitate sau marketing** al unității medicale (prin website spre exemplu) sau chiar al medicului (prin publicarea pe blogul personal a unor cazuri celebre care au fost tratate). Model de consimțământ găsiți în **Anexa 4 Consimțământ specific R.G.P.D.**

Același consimțământ se recomandă a fi utilizat și în situația în care, în calitate de medic, doriți să participați la un congre științific și **se dorește folosirea unor date care pot duce la identificarea persoanei** în mod direct sau indirect. În cazul în care materialele pe care le folosiți sunt anonimizate, adică nu mai este posibilă pe nici cale identificarea persoanei, nu se impune folosirea acestui consimțământ.

- **Exemplu**: prezentarea unui studiu de caz la un congres, care include detalii personale ale pacientului precum vârsta, sexul și istoricul medical, poate chiar și fotografii care pot duce în mod indirect (prin conectarea cu alte informații) la identificarea persoanei ar impune obținerea unui consimțământ.

Consimțământul acesta poate fi **atât în format letric (tipărit) cât și digital**. Alegeți forma care vă sprijină cel mai mult activitatea curentă.

- **Exemplu**: Utilizarea unui formular electronic de consimțământ pe o tabletă în loc de formular tipărit este la fel de validă! Aceasta ar presupune documentarea mai ușoară a consimțămintelor obținute spre deosebire de varianta tipărită.

Asigurați-vă că textul consimțământului este clar și ușor de înțeles pentru pacient, folosind un limbaj simplu și fără termeni tehnici sau jargon medical.

- **Exemplu**: O clinică stomatologică dorește să folosească datele pacienților pentru a trimite newslettere cu informații despre oferte speciale, promoții sau evenimente organizate de clinică. În acest scop, clinica trebuie să obțină consimțământul pacienților pentru prelucrarea datelor cu caracter personal în scopuri de marketing. Pentru a se asigura că textul consimțământului este clar și ușor de înțeles, clinica decide să folosească următorul limbaj simplu, fără termeni tehnici sau jargon medical:

- *"Ne dorim să vă ținem la curent cu ultimele noastre oferte și evenimente. Dacă sunteți de acord să primiți informații despre promoțiile noastre prin e-mail, vă rugăm să bifați căsuța de mai jos și să ne furnizați adresa de e-mail. Ne angajăm să păstrăm confidențialitatea datelor dumneavoastră personale și să le folosim doar în scopul menționat. În orice moment puteți alege să vă retrageți consimțământul și să nu mai primiți astfel de comunicări, urmând instrucțiunile din e-mailurile pe care le veți primi sau contactându-ne direct."*

Informați pacientul despre dreptul său de a-și retrage consimțământul în orice moment și asigurați-vă că acest proces este simplu și ușor accesibil.

- **Exemplu:** Vezi cazul de mai sus! Ce este de reținut este faptul că o persoană poate adresa pe orice canal o cerere de ștergere, chiar și verbal (ex. și apelul video este înregistrat) și trebuie să se țină cont de ea.

Documentați și păstrați în siguranță înregistrările privind consimțământul pacienților, pentru a putea demonstra conformitatea cu RGPD în cazul unui control sau al unei plângeri.

- **Exemplu**: Crearea unui sistem de arhivare securizat, fizic (dosare în fișete metalice) sau digital (foldere dedicate, registre în Microsoft Excel dedicate) pentru a păstra copii ale consimțământurilor semnate de pacienți.

Instruiți personalul care se ocupă de obținerea acestui consimțământ.

- **Exemplu**: Explicați-le faptul că ar trebui să invite pacientul pe un limbaj prietenos la oferirea consimțământului, faptul că acesta ar trebui documentat, faptul că ar trebui păstrat în condiții de siguranță fizică sau electronică ș.a.

Ce ar trebui să cunoașteți în materie de Rele practici:

A nu informa pacientul despre scopul prelucrării datelor cu caracter personal, despre consimțământ sau a omite informații esențiale legate de prelucrarea datelor în consimțământ.

- **Exemplu**: Publicăm pe pagina de blog o fotografie a unor analize medicale cu scopul de a detalia particularitățile unui caz studiat. Nu anonimizăm nimic, nu solicităm consimțământ.

- **Utilizarea unui limbaj ambiguu, confuz sau greu de înțeles** în consimțământul solicitat pacientului, făcând dificilă înțelegerea acestuia cu privire la drepturile sale și la modul în care datele sale vor fi prelucrate.
    - **Exemplu**: Folosirea unui formular foarte vast, greu de urmărit sau includerea tuturor aspectelor legate de consimțământ și prelucrarea datelor în scop de publicitate în Formularul de Acord Informat.

- **Încercarea de a obține consimțământul pacientului prin presiune, manipulare sau coerciție**, cum ar fi condiționarea oferirii serviciilor medicale de acordul pacientului pentru prelucrarea datelor în scopuri de marketing sau cercetare.
    - **Exemplu**: Se refuză consultul medical pentru lipsa semnării acordurilor specifice de marketing.

- **A nu respecta dreptul pacientului de a-și retrage consimțământul sau a face dificil sau neclar procesul de retragere a consimțământului**.
    - **Exemplu**: O persoană adresează un simplu email prin care solicită să îi fie șterse datele publicate pe website. Pentru că nu a folosit formularul specific pus la dispoziție de unitatea medicală, această solicitare este ignorată. Acest aspect reprezintă o încălcare.

- **A nu păstra în siguranță înregistrările** privind consimțământul pacienților și **a nu avea un sistem de gestionare a consimțământurilor** actualizat și eficient.
    - **Exemplu**: Nu este înregistrată în vreun registru electronic solicitarea de ștergere a unui consimțământ din baza de date de newsletter cu privire la serviciile oferite de clinica medicală. Acest fapt duce la transmiterea din nou a unor comunicări comerciale după adresarea unei cereri pe email cu privire la retragerea consimțământului.

- **A nu oferi instruire și sprijin adecvat personalului medical și administrativ** cu privire la protecția datelor și consimțământul pacienților, ceea ce poate duce la aplicarea incorectă a procedurilor și la încălcarea drepturilor pacienților.
    - **Exemplu**: Lipsa documentării instruirii printr-un proces verbal semnat de angajat poate atrage răspunderea angajatorului pentru o anumită situație, chiar dacă angajatorul susține că a realizat instruirea în cadrul unor ședințe de echipă, dar care nu au fost documentate.

Prin evitarea acestor rele practici vă veți asigura că abordați în mod corespunzător și eficient aspectele legate de consimțământ și prelucrarea datelor cu caracter personal, protejând astfel drepturile și intimitatea pacienților și evitând eventualele sancțiuni legate de încălcarea RGPD.

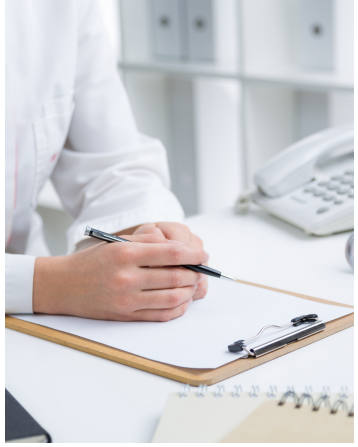
Cazuistică relevantă

Clinica ABC, specializată în tratamente de fertilitate, a realizat un studiu pentru a evalua eficacitatea unei tehnici inovatoare de fertilizare in vitro (FIV). În cadrul studiului, clinica a colectat și a analizat datele medicale ale cuplurilor care au beneficiat de această procedură FIV, cu scopul de a publica rezultatele pe site-ul propriu și în publicații de specialitate pentru a atrage noi pacienți.

Cu toate acestea, în procesul de colectare și analiză a datelor, clinica nu a obținut consimțământul pacienților pentru utilizarea informațiilor lor personale în scopul studiului și nu a implementat măsurile de anonimizare necesare. Astfel, rezultatele studiului, publicate pe site-ul clinicii și în articolele de specialitate, conțineau detalii personale ale pacienților, cum ar fi vârsta, sexul, istoricul medical și, în unele cazuri, chiar și inițialele acestora.

Unul dintre pacienții afectați a observat publicarea datelor sale personale și a înaintat o plângere către Autoritatea Națională de Supraveghere a Protecției Datelor. În urma anchetei, s-a constatat că nu au fost respectat prevederile RGPD privind obținerea consimțământului și anonimizarea datelor. Clinica a fost amendată, a trebuit să își retragă studiul și să notifice toți pacienții afectați despre încălcarea confidențialității datelor lor.

Acest incident ar fi putut fi evitat dacă Clinica ABC ar fi obținut consimțământul pacienților pentru prelucrarea datelor cu caracter personal în scopul studiului și ar fi implementat măsuri adecvate pentru a asigura anonimizarea datelor. Acest lucru ar fi protejat drepturile și intimitatea pacienților și ar fi evitat sancțiunile legate de încălcarea RGPD.





PARTEA a III-a | CAPITOLUL 4

PRELUCRAREA ȘI PROTECȚIA DATELOR ÎN SĂNĂTATE

De la cadrul legal la drepturile pacienților
Considerații pe larg

GHID DEZVOLTAT DE

ÎN COLABORARE CU GDPRComplet.ro

4.1 CADRUL LEGISLATIV ȘI APLICABILITATEA R.G.P.D.

Ce vă oferă această secțiune a Ghidului?

- Veți înțelege că activitatea medicală beneficiază de o protecție legislativă specială dintr-o perspectivă sectorială, distinctă de cea a realizării actului medical, pentru a proteja sănătatea și viața persoanelor. Această protecție specială are în centrul său **Datele Medicale și Viața privată** a persoanelor fizice.

- Veți înțelege că **activitatea medicală este îmbunătățită** dacă se realizează conform unor principii de protecție a datelor existente în legislația internațională și a Uniunii Europene.

- Veți înțelege că există riscuri mari pentru apărarea confidențialității dintre medici și pacienți, datorită **dezvoltării accelerate a tehnologiei**. Pe de altă parte, veți înțelege că protecția datelor medicale depășește sfera relației dintre medici și pacienți.

Datele privind starea de sănătate

Legislația de protecție a datelor, în special **Regulamentul General privind Protecția Datelor (R.G.P.D.)**, leagă această protecție a datelor medicale de **definirea concretă** a categoriei, pentru că o consideră o *categorie specială de date*, deosebindu-se de toate celelalte categorii, denumind-o date referitoare la sănătate. Este o categorie specială pentru că dezvăluirea datelor medicale poate evidenția aspecte din viața intimă a unei persoane, aspecte privind viața privată, personalitatea sa etc.

"Datele referitoare la sănătate" sunt toate datele cu caracter personal privind sănătatea fizică sau mentală a unei persoane fizice, inclusiv furnizarea de servicii de asistență medicală, care dezvăluie informații despre starea de sănătate trecută, actuală și viitoare a acestei persoane (*Recomandarea CM/Rec(2019)2 a Comitetului de Miniștri către statele membre privind protecția datelor referitoare la sănătate*).

Sintetizând, în activitatea sa, un medic trebuie să țină cont că datele medicale:

- sunt atât cele referitoare la sănătatea sa fizică, cât și la cea mentală
- sunt atât datele prelucrate în procesul de intervenție, cât și de tratament sau în cadrul serviciilor de asistență medicală
- sunt atât datele privind trecutul medical al unei persoane, precum și datele actuale sau care vizează sănătatea viitoare a unei persoane

R.G.P.D. declară datele medicale ca având o natură sensibilă, deosebindu-se de majoritatea altor date cu caracter personal; de asemenea, aceste date sunt însoțite de riscuri mai mari asupra vieții private a unei persoane sau asupra altor drepturi și libertăți. Pentru aceste motive R.G.P.D. le conferă o protecție specială, mai accentuată și mai ridicată față de alte date personale.

! Notă: Aceeași protecție specială este acordată datelor genetice și datelor biometrice, indiferent că se referă sau nu la starea de sănătate.

Nucleul juridic al protecției legale a datelor medicale îl reprezintă Regulamentul General privind Protecția Datelor, acesta fiind obligatoriu de respectat de către România și de fiecare stat membru al Uniunii Europene.

Care sunt principalele consecințe ale faptului că R.G.P.D. este nucleul juridic al protecției legale?

- În primul rând, orice activitate medicală și, totodată, orice legislație specială sau sectorială prin care se stabilesc reguli pentru activități în legătură cu date medicale trebuie să respecte **cel puțin nivelul de protecție stabilit de R.G.P.D.**
    - **Exemplu** relevant prin simplitatea acestuia și prin specificitatea în legătură cu activitatea medicală: deșeurile medicale, cum ar fi cele anatomo-patologice reprezentate de fragmente din organe și organe umane, părți anatomice, trebuie gestionate nu doar cu grija principală a menținerii la locul desfășurării activității medicale a condițiilor de igienă și a prevenirii răspândirii oricăror boli sau a prevenirii oricăror riscuri specifice medicale; prelucrarea acestora trebuie să se realizeze și cu respectarea minimă a regulilor de protecție a datelor personale, prevăzute de R.G.P.D.. Această din urmă protecție legală va adăuga la obiectivele de sănătate și igienă ce trebuie atinse în activitatea medicală un obiectiv specific: protecția persoanei despre a cărei date genetice și de sănătate ar fi vorba împotriva oricărei tentative de acces neautorizat la acestea, de sustragere a unor asemenea date, de punere în pericol a propriilor țesuturi și organe ori chiar de vătămare a reputației sau de abuz din partea unor privați sau din partea unor autorități ale statului. Spre exemplu, în absența unei protecții speciale, un fragment de țesut ar putea fi utilizat în așa fel încât să se „planteze” în interiorul scenei unei infracțiuni, atrăgând posibile consecințe juridice de natură penală pentru persoana pe care proba biologică o va identifica în mod unic.

- A două consecință principală a faptului că R.G.P.D. este nucleul juridic al protecției legale constă în aceea că prin legislația specifică unei activități **se pot introduce măsuri și mai drastice de protecție a datelor medicale.**
    - Spre **exemplu**, prelevarea de către personalul medical a unor probe biologice de la unele persoane care au săvârșit anumite infracțiuni, cu scopul introducerii profilului genetic într-o bază de date, se va realiza cu respectarea prevederilor Legii nr. 76/2008 privind organizarea și funcționarea Sistemului Naţional de Date Genetice Judiciar, lege care, cel puțin în teorie, ar trebui să respecte cel puțin nivelul de protecție specială prevăzut de R.G.P.D. (ori, după caz, de Legea 363/2018), dar care va cuprinde și alte garanții suplimentare legate de perioada specifică de stocare a datelor, de asigurarea securității și confidențialității bazei de date și alte asemenea.

Întrebări legitime care apar ori de câte ori un medic sau orice personal de specialitate asociat cu activități medicale și de sănătate este pus în situația de a face față legislației de protecție a datelor medicale

- O întrebare este **dacă este necesar să cunoască întreagă această legislație**. Răspunsul la această întrebare este negativ, deoarece acesta este un obiectiv foarte dificil chiar și pentru specialiștii care lucrează strict pe domeniul protecției datelor, iar personalul medical și din sănătate are misiunea specifică de a acorda îngrijiri medicale sau a furniza servicii medicale. Este foarte adevărat că un asemenea răspuns nu ar fi pe gustul unei părți a juriștilor care vor contraargumenta invocând principiul latin Nemo censetur ignorarem legem (Nimeni nu se poate scuza de necunoașterea legii). Pentru a se ajunge la o soluție realistă activitățile medicale trebuie să cuprindă standardul de protecție a datelor în mod firesc datorită cuprinderii acestuia în mod organic încă din perioada învățării cel puțin la nivelul studiilor de licență efectuate de viitorii medici; totodată, prin instruiri de bază care să se focalizeze practic asupra acestui standard. Inclusiv rolul prezentului ghid este de instruire de bază. În concluzie, conștientizarea de către personalul care lucrează cu date medicale asupra standardului de protecție a datelor este etapa cea mai importantă pentru obiectivul protecției acestora.

- În rândul întrebărilor legitime, apare și o alta: anume, **unde se percepe cel mai concret protecția datelor medicale în acest sector?** Răspunsul este extrem de simplu: în managementul oricărei activități care se intersectează direct sau indirect cu date cu caracter personal medicale. Spre exemplu, dacă am pe un calculator aplicația cu dosarul medical electronic trebuie să îmi iau măsuri foarte precise de protecție a securității și siguranței dispozitivului, astfel încât să previn orice acces neautorizat la acele baze de date ori distrugerea acestora. Situația poate fi și mai „vie”! Spre exemplu, atunci când consult un pacient pentru a stabili un diagnostic, mă voi asigura că această activitate nu permite unui terț „spectator”, aflat în proximitate, să identifice persoana respectivă și să obțină date privind sănătatea acesteia, utilizând pentru aceasta un telefon mobil cu funcții de înregistrare audio/video. Situația este asemănătoare, chiar dacă este supusă unor riscuri și mai mari, atunci când consultația se desfășoară online. Medicul se va asigura că la celălalt terminal se află doar beneficiarul consultației și nu alte persoane. În același timp, medicul se va asigura că în proximitatea sa fizică, la momentul transmisiei, se află doar personal autorizat și, recomandabil, instruit în domeniul protecției datelor.

- O altă întrebare legitimă în legătură cu această legislație de protecție a datelor este aceea care lămurește rostul ei mai ales pentru activitatea unui medic și a oricărei alte persoane care prelucrează date medicale. **Pentru ce avem o asemenea legislație?** Activitatea medicală nu reprezintă o activitate desprinsă de ființa umană sau o profesie care tratează niște obiecte. În centrul acesteia se găsește o ființă vie, o persoană fizică. Legislația de protecție a datelor personale transformă activitatea medicală din una axată strict pe cunoștințele de specialitate ale medicului în una complet bilaterală și multisocială, bazată pe **etică**. Protecția datelor în orice profesie, indiferent că este una medicală sau de altă natură, înseamnă **etică**, contribuind la prezervarea demnității, la apărarea tuturor drepturilor și libertăților persoanelor.

- În mod firesc, problema respectării sau nerespectării legislației de protecție a datelor aduce cu sine întrebarea referitoare la **care ar putea fi consecințele nerespectării acestei legislații și cine le suportă**. Răspunsul poate fi complex, dar în esență trebuie știut că nerespectarea acestei legislații poate „îmbrăca" foarte multe forme, poate să se exprime prin infinit de multe situații și să privească multe entități: medic, personalul medical, angajatorul acestuia, personalul auxiliar, furnizorul de servicii medicale, furnizorul de dispozitive medicale etc. Medicul este interesat în primul rând pentru că nerespectarea principiilor poate conduce la unele forme de malpraxis medical, care pentru pacient semnifică încălcarea vieții sale private, uneori vătămarea vieții și integrității sale fizice și/sau psihice. Spre exemplu, absența consemnării cu exactitate a unor date medicale care țin de stabilirea unui diagnostic, manipularea ulterioară greșită a acestora poate conduce la o intervenție eronată asupra unui pacient. Este foarte adevărat că, sub aspectul strict al regulilor de protecție a datelor, va exista o consecință aparte, complementară, de cele mai multe ori pentru angajator, deoarece acesta trebuie să se asigure că se respectă toate regulile de protecție a datelor într-o unitate spitalicească. Explicația va fi detaliată în următoarele secțiuni, atunci când se va analiza principiul responsabilității pentru prelucrarea datelor personale.

- În final, fără însă a epuiza toate posibilele întrebări legitime, apare o întrebare ca urmare a tuturor afirmațiilor de mai sus. Cum ar putea un medic, care nu cunoaște complet toate reglementările din domeniul protecției datelor, să le și respecte, mai ales că toate activitățile sale sunt atât de variate, fac parte dintr-un ansamblu organizatoric (spre exemplu, lucrează într-un spital) și sunt exprimate prin nenumărate modalități (în

baze de date, în activități directe de tratament sau alte îngrijiri, în componente organice și anorganice, în fișe și comunicări electronice, în înregistrări audio/video etc.). Răspunsul se bazează pe doi piloni obligatorii: **primul pilon este instruirea și conștientizarea standardului de protecție**, pilon amintit; **al doilea pilon**, presupune recurgerea de către organizația în care se desfășoară orice activități de genul celor care presupun utilizarea datelor medicale, la un specialist în domeniul protecției datelor, **specialist care să asigure implementarea standardului de protecție a datelor și a conformității cu R.G.P.D.** în activitățile organizatorice și de management ale organizației. **Prezentul ghid are rolul în special de a contribui la realizarea primului pilon, fără însă a se reduce la acesta**. O mențiune extrem de importantă în ideea răspunsului la această întrebare este aceea că protecția datelor privită în ansamblul său presupune și un **al treilea pilon** de urmărit: **conștientizarea și instruirea persoanelor fizice vizate, adică a pacienților.**

Cunoașterea R.G.P.D. de către destinatarii acestui ghid se va face prin prezentarea sistematică a celor **7 principii de protecție a datelor,** deoarece în acest mod se poate înțelege cu ușurință standardul de protecție a datelor și se poate aplica în activitatea de zi cu zi.

1 Primul principiu este denumit **principiul legalității, echității și transparenței** și va fi analizat distinct pe fiecare dintre cele trei componente care îl caracterizează. Chiar dacă este mai dificil de aplicat, cel mai ușor de înțeles de către un medic este **principiul legalității**, deoarece orice medic cunoaște „organic” că toate activitățile pe care le realizează trebuie să fie prevăzute și în conformitate cu legea. Astfel, acest principiu al legalității semnifică ideea că ori de câte ori activitatea medicului presupune interferența cu date medicale ale unei persoane fizice, prelucrarea acelor date trebuie să corespundă clar unei situații pe care legea a avut-o în vedere. În caz contrar, prelucrarea datelor medicale personale nu are voie să se realizeze. Aceasta este o interdicție stipulată de norma juridică, mai exact **Articolul 9 aliniatul 1 din R.G.P.D.**

Ce anume va face un medic pentru a respecta acest principiu al legalității? Trebuie să se asigure că activitatea sa de prelucrare a datelor *se potrivește uneia dintre următoarele situații în care este permisă prelucrarea datelor medicale*, situațiile fiind strict prevăzute de articolele 6 și 9 din R.G.P.D.: atunci când există consimțământul explicit al persoanei despre ale cărei date personale este vorba (denumită specific persoana vizată), atunci

când este necesară prelucrarea datelor medicale în scopuri de medicină preventivă, pentru diagnosticare, pentru acordarea îngrijirilor medicale sau a tratamentului medical, ori prelucrarea este necesară pentru administrarea serviciilor medicale.

1.1 **CONSIMȚĂMÂNTUL EXPLICIT** este una dintre condițiile care, odată îndeplinite, asigură Legalitatea unei prelucrări de date medicale.

Definiția prevăzută de R.G.P.D.: „consimțământ" al persoanei vizate înseamnă *orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate* prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate (Art. 4 lit.11 R.G.P.D.).

Pentru a fi **specific**, consimțământul trebuie să fie dat în legătură cu o situație concretă de prelucrare a datelor medicale, o situație conturată și precizată clar. Încălcarea acestei cerințe se produce cel mai adesea prin solicitări de consimțământ extrem de generalizate și evazive, sub forma unor acorduri pur teoretice și formalizate.

Exemplu de practică greșită:

Acord/Consimțământ al Persoanei Vizate

Subsemnatul(a) _____ [Numele și prenumele pacientului], născut(ă) la data de _____ [data nașterii], domiciliat(ă) în _____ [adresa], posesor al actului de identitate seria _____, nr. _____, eliberat de _____, la data de _____, îmi exprim acordul/consimțământul pentru prelucrarea datelor mele medicale de către _____ [Numele și adresa clinicii/centrului medical/furnizorului de servicii medicale].
Sunt de acord ca datele mele medicale să fie prelucrate în vederea obținerii unor informații despre sănătatea mea și în scopuri generale de cercetare.
Data: _____ Semnătura: _____

În acest exemplu, consimțământul este vag și nu explică în mod clar scopurile pentru care datele medicale vor fi prelucrate. Acesta menționează "scopuri generale de cercetare", dar nu oferă detalii despre ce tip de cercetare sau cum vor fi folosite datele în acest context. Astfel de consimțământ nu respectă principiul specificității, conform Regulamentului General privind Protecția Datelor (GDPR).

Consimțământul informat presupune înțelegerea de către persoana vizată a unor aspecte relevante în legătură cu prelucrarea datelor sale medicale, înțelegere datorată comunicării pe care o are cu operatorul datelor. Pacientul trebuie să înțeleagă, pe baza informării realizate la momentul solicitării consimțământului, **ce tipuri de date i se prelucrează, care este scopul pentru care acele date se prelucrează, cine îi va utiliza acele date, ce drepturi are în legătură cu prelucrarea datelor sale, ce se întâmplă dacă nu este de acord cu prelucrarea datelor sale**. Pentru a se atinge acest obiectiv comunicarea dintre medic sau personalul autorizat trebuie să se realizeze într-o manieră corectă, într-o formă inteligibilă și să acopere toate aspectele relevante.

- **Exemplu de practică greșită și sancțiunea aplicată:** *Utilizarea datelor medicale dintr-un dosar de angajare pe un post cu prilejul unei alte angajări, în loc să se realizeze o nouă reexaminare medicală în vederea angajării, reprezintă o prelucrare abuzivă a datelor medicale, caracterul abuziv fiind accentuat mai ales în condițiile în care persoana vizată nu a fost informată în vreun fel la momentul întocmirii primului dosar de angajare că asemenea date ar putea fi utilizate și în eventualitatea unor noi proceduri de recrutare. Cauza relevantă privind încălcarea acestei reguli a consimțământului informat este* ***V. și EDPS împotriva Parlamentului European****, persoanei vizate acordându-i-se despăgubiri morale de 20 000 Euro.*

Consimțământul explicit presupune stabilirea clară că pacientul a acceptat prelucrarea datelor sale medicale în legătură cu toate activitățile de prelucrare a datelor sale medicale care se vor realiza pe baza acestuia. Chiar dacă nu este necesar întotdeauna un consimțământ scris, trebuie să rezulte cel puțin din circumstanțele unei situații că această atitudine de acceptare este clară, ceea ce dintr-un unghi al dreptului, echivalează cu un acord al persoanei vizate.

- **Exemplu de practică greșită și sancțiunea aplicată**: *În cazurile în care, datorită circumstanțelor, se justifică transmiterea de către un spital a datelor referitoare la starea de sănătate, tratamentul acordat unui pacient și alte informații medicale detaliate către angajatorul acelui pacient,* ***această posibilă transmitere trebuie să fi fost consimțită de pacient la momentul solicitării sale de a primi îngrijiri medicale.*** *Un spital nu este obligat să ofere unui angajator informații detaliate privind starea de sănătate a unui pacient, în absența consimțământului explicit al acestuia.*

*O cauză relevantă este **Radu împotriva Republicii Moldova**, în care Curtea europeană a drepturilor omului a constatat încălcarea vieții private a pacientului, deoarece spitalul căruia angajatorul îi solicitase informații privind concediul medical acordat, a comunicat date medicale în absența vreunui consimțământ explicit al persoanei vizate. S-au acordat 4500 Euro despăgubiri morale.*

Consimțământul liber presupune un acord al pacientului de a fi prelucrate datele sale personale, iar acest acord este determinat de o alegere reală și un control real din partea persoanelor pacienților. Ca regulă generală, R.G.P.D. prevede că, dacă persoana vizată nu beneficiază de o alegere reală, dacă se simte obligată să consimtă sau dacă va suporta consecințe negative în cazul în care nu consimte, atunci consimțământul nu va fi valabil. Dacă consimțământul este înglobat, ca parte ce nu poate fi negociată, în cuprinsul termenelor și condițiilor, se prezumă că acesta nu a fost exprimat în mod liber. În consecință, consimțământul nu va fi considerat liber exprimat dacă persoana vizată nu este în măsură să refuze sau să-și retragă consimțământul fără a fi prejudiciată.

- **Exemplu de practică greșită și sancțiunea aplicată:** *O persoană se prezintă la o clinică privată pentru a efectua un control de rutină. După ce discută cu medicul și completează formularul de istoric medical, asistenta îi oferă un formular de consimțământ în legătură cu prelucrarea datelor sale medicale. În formular se precizează că datele pacientului pot fi prelucrate și partajate cu companii terțe pentru cercetare, marketing și dezvoltarea de noi tratamente. Persoana nu este confortabilă cu ideea de a-și împărtăși datele medicale cu companii terțe și își exprimă îngrijorarea față de asistentă. Asistenta îi spune că, dacă nu semnează formularul de consimțământ, nu va putea primi serviciile medicale oferite de clinică. În acest caz, consimțământul nu este liber, deoarece persoana vizată se simte constrânsă să semneze formularul pentru a primi îngrijirea medicală necesară. În cauza **Dent Estet Clinic SA** s-a aplicat o sancțiune de 1000 de EURO deoarece un medic stomatolog colaborator a prelucrat, inclusiv prin utilizare și dezvăluire, datele personale privind starea de sănătate a persoanei vizate, în cadrul unui articol postat pe blogul personal, fără să prezinte dovezi privind obținerea consimțământului expres al persoanei implicate și fără informarea sa prealabilă.*

Notă! Practic și ușor de înțeles, dacă un medic sau o altă persoană dorește să afle mai multe despre cum anume trebuie să funcționeze o relație dintre el și un pacient, pe baza consimțământului, are la dispoziție un document bine realizat și care îmbracă forma unor îndrumări oficiale în această privință, deoarece ele sunt elaborate de un organism de expertiză relevant în domeniul protecției datelor, anume Comitetul European pentru protecția datelor. Documentul este intitulat **Orientările nr 05/2020 privind consimțământul în temeiul Regulamentului 2016/679.**

1.2 Date prelucrate în legătură directă sau indirectă cu desfășurarea muncii!

Prelucrarea datelor medicale se realizează pentru că este necesară în scopul îndeplinirii obligațiilor și al exercitării unor drepturi specifice operatorului sau persoanei vizate în domeniul ocupării forței de muncă și al securității sociale și protecției sociale, în măsura în care acest lucru este autorizat de dreptul Uniunii sau de dreptul intern, ori de un acord colectiv de muncă încheiat în temeiul dreptului intern care prevede garanții adecvate pentru drepturile fundamentale și interesele persoanei vizate (Articolul 9(2) lit.b R.G.P.D.). Asemănător, prelucrarea este legală dacă este necesară **în scopuri legate de medicina preventivă sau a muncii,** de evaluarea capacității de muncă a angajatului, de stabilirea unui diagnostic medical, de furnizarea de asistență medicală sau socială sau a unui tratament medical sau de gestionarea sistemelor și serviciilor de sănătate sau de asistență socială (Articolul 9 litera h R.G.P.D.).

Situația de mai sus acoperă tipologii de cazuri de prelucrare a datelor în scopuri variate. Câteva exemple mai des întâlnite sunt redate mai jos:

- **Evaluarea capacității de muncă**: Înainte de angajare, un angajator poate solicita un control medical pentru a evalua dacă un potențial angajat este apt din punct de vedere medical să îndeplinească sarcinile aferente postului. Datele medicale colectate în acest scop sunt utilizate pentru a lua decizii privind angajarea și adaptarea la condițiile de muncă pentru care a fost recrutat sau angajat.

- **Evaluarea necesității de a acorda concediu medical**: Angajatorii prelucrează datele medicale ale angajaților pentru a determina dacă un angajat are dreptul la concediu medical în caz de boală sau accident. Aceasta implică adesea obținerea unui certificat medical de la medicul angajatului și, în unele cazuri, solicitarea unei evaluări medicale independente.

- **Evaluarea eligibilității pentru beneficii de securitate socială și protecție socială**: Agențiile guvernamentale responsabile de administrarea programelor de asistență socială pot prelucra datele medicale pentru a evalua eligibilitatea unei persoane pentru beneficii, precum pensia de invaliditate, indemnizația de handicap sau ajutorul financiar pentru îngrijirea copiilor cu dizabilități.

- **Reintegrarea pe piața muncii a persoanelor cu dizabilități sau probleme de sănătate**: Programele de reintegrare profesională, cum ar fi cele finanțate de guvern sau de organizații non-profit, pot utiliza datele medicale pentru a identifica nevoile specifice ale persoanelor cu dizabilități sau probleme de sănătate și a adapta serviciile oferite în consecință.

- **Evaluarea riscurilor la locul de muncă**: Angajatorii pot prelucra datele medicale pentru a evalua și a controla riscurile de sănătate și securitate la locul de muncă, cum ar fi expunerea la substanțe periculoase, condiții de muncă stresante sau zgomotoase.

- **Stabilirea situațiilor medicale asigurate:** Societățile de asigurare pot prelucra unele date medicale, pentru a stabili dacă asigurarea medicală acoperă cazul asigurat și a acorda beneficiile financiare rezultate în urma contractului de asigurare.

Notă! Toate aceste exemple presupun prelucrarea datelor cu caracter medical într-un mod care respectă drepturile și interesele persoanelor vizate, precum și reglementările legale și de confidențialitate aplicabile. Nu este necesar consimțământul persoanei în legătură cu prelucrările de acest fel, însă situațiile de prelucrare trebuie foarte atent realizate și trebuie verificată existența garanțiilor specifice unei protecții speciale, cum este cazul informării pacietului, adică a persoanei vizate.

1.3 Datele medicale pot fi prelucrate dacă este necesar pentru **protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice**, atunci când persoana vizată se află în incapacitate fizică sau juridică de a-și da consimțământul.

Această situație trebuie să fie receptată ca una complet de excepție, specifică unor situații de cele mai multe ori extrem de grave, astfel că sunt mai rar întâlnite în activitățile medicale curente, cu excepția serviciilor medicale de urgență.

- *Un **exemplu** este cazul când o persoană aflată în stare de inconștiență nu poate consimți în privința prelucrării datelor sale, astfel că personalul de specialitate care are nevoie de istoricul său din dosarul electronic de sănătate poate să facă aceasta deoarece urmărește protejarea unor interese esențiale ale pacientului. Aceeași situație este valabilă când persoana vizată deși nu este în stare de inconștiență, are nevoie urgentă de un tratament pentru protejarea intereselor sale esențiale privind sănătatea, dar nu are nici discernământ deplin, nici nu există vreo persoană autorizată de lege prezentă pentru a consimți în numele acesteia.*

- Un **exemplu** diferit este acela când este necesară protecția intereselor vitale ale unei alte persoane fizice decât aceea ale cărei date sunt prelucrate. Această situație este extrem de delicată deoarece presupune dezvăluirea datelor medicale către terți, dar are de multe ori fundamente etice la bază. *Probabil cea mai cunoscută cauză jurisprudențială este cauza **Tatiana Tarasoff** care evidențiază necesitatea dezvăluirii de către un medic (sau o altă persoană supusă obligației de confidențialitate) a unor date medicale obținute în regim de confidențialitate de la pacient, dacă informațiile respective sunt necesare pentru a proteja interesele vitale ale unui terț sau chiar ale unei comunități. Iată succint ideea: un pacient la o clinică vă dezvăluie că dorește să omoare pe cineva. Sunteți supus confidențialității: totuși, dacă vi se pare rezonabilă rezoluția, raportat la boală, la istoricul persoanei, la context, trebuie să anunțați autoritățile de aplicare a legii, chiar dacă aceasta înseamnă o încălcare a confidențialității absolute.*

Notă! Această situație a protejării intereselor vitale nu poate fi transformată într-o regulă generală a acordării îngrijirilor medicale sub pretextul că acestea contribuie oricum la apărarea sănătății persoanelor.

1.4 Dacă prelucrarea datelor medicale se realizează de către un organism fără scop lucrativ, dar cu specific politic, filozofic, religios sau sindical, atunci o asemenea prelucrare ar putea fi legală când îndeplinește următoarele condiții (Art.9 lit.d R.G.P.D.):

- prelucrarea să se refere numai la membrii sau la foștii membri ai organismului respectiv sau la persoane cu care acesta are contacte permanente în legătură cu scopurile sale
- datele cu caracter personal să nu fie comunicate terților fără consimțământul persoanelor vizate
- activitățile de prelucrare sunt legitime și însoțite de garanții adecvate

Una dintre cauzele ilustrative privitoare la această situație este **cauza Bodil Linquist**, deoarece evidențiază că unele date medicale pot fi prelucrate de către o asociație cu privire la membrii săi, dar nu pot fi dezvăluite terților decât pe bază de consimțământ.

1.5 Datele medicale pot fi prelucrate și în situația în care ele **sunt făcute publice în mod manifest de către persoana vizată** (articolul 9 lit.e R.G.P.D.).

Câteva **exemple** sunt ilustrative:

- **Postări pe rețelele de socializare**: Dacă o persoană își publică numele, adresa de e-mail, numărul de telefon sau alte informații personale, inclusiv date medicale, pe platforme precum Facebook, Instagram, Twitter sau LinkedIn, acestea sunt considerate date făcute publice în mod manifest.

- **Participarea la evenimente și conferințe**: Persoanele care participă la evenimente publice și unele aspecte care privesc sănătatea lor pot fi percepute clar de către terți (ex. are un picior amputat expus în mod clar) fac publice aceste informații în mod manifest.

- **Testimoniale și recenzii online**: Când o persoană oferă un testimonial sau o recenzie pentru un produs sau serviciu și își publică numele, fotografia și alte detalii personale, printre care date referitoare la starea sa de sănătate, aceste informații sunt considerate făcute publice în mod manifest.

Notă! Este extrem de important să se înțeleagă că această situație este legală doar dacă datele sunt postate chiar de către persoana vizată, nu de către un terț! Transmiterile de date medicale dezvăluite public în mod nelegal de către terți, alții decât persoana vizată, adică pacientul, pot fi ilegale dacă afectează viața privată a acestuia.

1.6 Este legală și prelucrarea datelor medicale dacă prelucrarea este necesară pentru constatarea, exercitarea sau **apărarea unui drept în instanță sau ori de câte ori instanțele acționează în exercițiul funcției lor judiciare** (Art.9 lit.f R.G.P.D.).

Cel mai adesea enunțul de mai sus acoperă situații în care instanțele de judecată solicită unor spitale documentație medicală privind un pacient, în interesul realizării unor probațiuni de care depinde soluționarea procesului, ori solicită unor experți medicali analiza unor date medicale sau furnizarea unor opinii medicale.

Dintr-o perspectivă practică trebuie știut că simpla întreprindere / inițiativă a unor demersuri cu conotații judiciare nu justifică o prelucrare a datelor medicale fără a avea vreo limitare a posibilităților de prelucrare sau a modalităților de prelucrare.

Exemple de rea practică:

- o instanță reproduce, în cadrul unei hotărâri de divorț, un extras din fișa medicală personală a pacientului deși nu era necesară ca probă *(L.L. c. Franței)*
- un act normativ, administrativ sau judiciar care limitează la zece ani perioada de confidențialitate a probelor produse care conțin date medicale, deși această perioadă nu era suficientă pentru protecția adecvată a vieții private a persoanelor în cauză (*Z v. Finlanda*)
- se permite divulgarea de date psihiatrice confidențiale privind un solicitant în timpul unei audieri publice, cu toate că o constatare judiciară se putea realiza în ședință confidențială (*Panteleyenko c. Ucrainei*)
- se face dezvăluirea identității unei persoane și a statutului de seropozitiv al acesteia într-o hotărâre judecătorească comunicată presei (*Z v. Finlanda*)

Notă! În aceeași idee a apărării unor drepturi, într-o formulă contencioasă, chiar dacă nu se ajunge întotdeauna în fața instanței de judecată, prelucrarea datelor medicale se poate realiza de către comisiile de specialitate care investighează cazurile de malpraxis medical. Întotdeauna trebuie ca datele medicale care se prelucrează să fie adecvate pentru scopul urmărit și prelucrarea datelor să fie balansată adecvat cu drepturile pacientului.

1.7 Prelucrarea datelor medicale este legală când se face **pentru motive de interes public major sau din motive de interes public în domeniul sănătății publice**, cum ar fi protecția împotriva amenințărilor transfrontaliere grave la adresa sănătății sau asigurarea de standarde ridicate de calitate și siguranță a asistenței medicale și a medicamentelor sau a dispozitivelor medicale (Art.9 lit. g și i R.G.P.D.).

Prelucrarea în asemenea situații necesită:

- existența unei legi naționale sau a unei legi a Uniunii Europene
- respectarea obligațiilor de confidențialitate
- garanții specifice pentru protejarea drepturilor persoanei vizate

Astfel de exemple pot fi întâlnite în România în perioada pandemiei COVID-19:

- impunerea întocmirii unor evidențe cu temperatura tuturor persoanelor care intră într-un magazin sau care vin la locul de muncă. Blocarea accesului acelora care au peste 37.3 C.
- impunerea unor declarații cu privire la locul în care te duci, permis specific doar prin ordonanță: Ex. la locul de muncă, la farmacie, la rude pentru îngrijiri medicale ș.a. Aceste declarații și datele existente pe ele erau verificate de polițiști care aveau acces în mod direct. Uneori s-a întâmplat să se fotografieze de către polițiști cu telefoanele personale, contrar bunelor practici! A.N.S.P.D.C.P. a intervenit cu un comunicat de presă prin care a adus clarificări asupra limitelor în care se poate desfășura această activitate.

1.8 Prelucrarea datelor medicale când este necesară **în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice** este permisă (Art.9 lit. j), însă trebuie să se facă cu respectarea următoarelor condiții:

- existența unei legi naționale sau a unei legi a Uniunii Europene
- respectarea obligațiilor de confidențialitate
- garanții specifice pentru protejarea drepturilor persoanei vizate

Notă: situațiile sunt expuse exact în litera legii, în realitate veți ține cont de următoarele:

- în scopuri de cercetare științifică este necesar consimțământul persoanei vizate - a se vedea **Orientarea 3.13 privind utilizarea datelor cu caracter personal în scopuri secundare decât cele în care au fost colectate inițial**
- în scopuri statistice este necesar consimțământul persoanei vizate, cu excepția situației când datele pot fi anonimizate, adică nu pot fi nicidecum legate de identitate unei persoane fizice - a se vedea **Orientarea 3.16 privind obținerea și gestionarea consimțământului persoanei vizate**
- în scopuri de arhivare în interes public, realitatea este că legea este temeiul prelucrării lor

2 Principiul legalității prelucrării datelor cu caracter personal presupune și **echitate și transparență** chiar dacă aceste ultime două valențe pot fi analizate distinct. Aceste valențe trebuie asigurate în virtutea regulilor R.G.P.D. însă ele sunt detaliate în mod specific în convențiile și actele internaționale privind bioetica, reprezentând principii a căror respectare va conduce și la asigurarea legalității. Acestea sunt prezentate în cele ce urmează.

2.1 **Autonomie**

Acest principiu presupune o autonomie a fiecărui individ și are printre consecințe / valențe următoarele:

- obligația de a obține **consimțământul liber și în cunoștință de cauză** de la o persoană, înainte de orice intervenție medicală sau de administrarea oricărui tratament
- posibilitatea persoanei de a-și **retrage consimțământul**
- dreptul de **informare asupra stării propriei sănătăți** și asupra rezultatelor testelor predictive
- „dreptul de a nu cunoaște”
- dreptul **persoanele incapabile** să ofere un consimțământ valabil de a fi **protejate**

2.2 **Binefacere și Non-maleficiență**

Presupune o **obligație morală** referitoare la **activitățile de îngrijire a sănătății și de cercetare** asupra ființelor umane sau în legătură cu ființele umane, obligație care presupune desfășurarea activităților în scopul **maximizării beneficiilor** și **reducerii** la maximum a **consecințelor negative** asupra persoanei fizice.

2.3 **Echitate**

Principiul impune ca activitățile din domeniul **asistenței medicale și a cercetării** să se desfășoare pe **baze corecte și echitabile.**

2.4 **Principiul Consimțământului Informat**

Persoana trebuie să aibă posibilitatea reală de a alege, iar nu a completa un formular și în realitate de a nu avea vreo posibilitate reală de decizie; pentru aceasta trebuie să fie corect informată asupra opțiunilor, asupra mecanismelor de acordare a asistenței sau tratamentului și asupra consecințelor, anterior petrecerii/producerii acestora.

2.5 **Protecția vieții private** (articolul 10)
Orice intervenție asupra elementelor biologice ale ființei umane poate fi realizată doar ținându-se cont de respectarea integrității fizice și psihice a persoanei fizice și cu consimțământul ori după caz informarea acesteia.

2.6 **Protejarea persoanelor care nu au capacitatea de a consimți** (articolul 6)
Presupune că acordarea tratamentului persoanelor din această categorie, spre exemplu minorilor, poate fi realizată numai dacă aduce beneficii reale și directe sănătății lor, ținând cont adecvat de dorințele respectivelor persoane și cu autorizarea reprezentanților legali.

2.7 **Respectarea demnității** (articolul 1)
Principiul demnității este la baza sistemului reglementar al Convenției de la Oviedo și interzice tratarea ființei umane într-un alt mod decât cel situat pe locul 1 în priorități, astfel încât armonia relațiilor indivizilor în societate, valorizarea lor proprie să nu fie deteriorate, iar avantajele biomedicinei să nu fie guvernate de pragmatism și câștiguri financiare sau de altă natură decât cele pentru propășirea societății umane.

2.8 **Preeminența ființei umane**
Acest principiu presupune că ființa umană se bucură de preeminență (prioritate și supremație) față de interesul exclusiv al științei sau al societății.

2.9 **Interzicerea câștigului financiar**
Organele și țesuturile, inclusiv sângele, nu ar trebui să fie cumpărate sau vândute sau să genereze câștiguri financiare pentru persoana de la care au fost prelevate sau pentru o persoană sau întreprindere terță. Comercializarea medicamentelor sau dispozitivelor medicale care conțin țesuturi umane ce au fost supuse unui proces de fabricație nu este interzisă, atâta timp cât țesutul folosit ca materie primă nu este vândut ca atare. Nu sunt permise plățile legate de obținerea consimțământului sau de autorizarea donării organelor/țesuturilor de la persoanele în cauză. Cu toate acestea, o persoană de la care a fost prelevat un țesut sau organ poate primi o compensație care nu constituie o remunerație, în schimb îl despăgubește în mod echitabil pentru cheltuielile suportate sau pierderea veniturilor.

2.10 **Principiul Nediscriminării**

Se interzice orice discriminare întemeiată pe patrimoniul genetic al unei persoane.

2.11 **Principiul respectării Standardele profesionale**

Orice intervenție în domeniul sănătății, inclusiv cercetarea, trebuie să fie efectuată în conformitate cu obligațiile și standardele profesionale relevante.

NOTĂ FINALĂ! Această parte a ghidului urmărește să pregătească medicul, profesionistul pentru înțelegerea semnificației datelor cu caracter personal ale pacienților utilizate în mod inerent în activitățile medicale, insistându-se pe relevanța etică și juridică.

4.2 LOCUL DREPTULUI LA PROTECȚIA DATELOR MEDICALE ÎN SISTEMUL JURIDIC

Înțelegerea domeniului protecției datelor cu caracter personal trebuie să aibă printre punctele esențiale de pornire **spectrul internațional.** Protecția datelor personale nu poate fi desprinsă, în primul rând faptic, de spectrul internațional, deoarece chiar dacă locul colectării unor date este situat doar într-un anumit areal geografic, supus unei jurisdicții naționale, necesitățile de utilizare a respectivelor date și potențialul extrem de ridicat de circulație/transfer cu viteză a respectivelor date, la distanțe mari, impun în realitate ca protecția datelor personale să se realizeze într-un plan internațional. Posibilitățile de reglementare internațională regională (la nivel continental sau unional) sunt mai eficiente, însă, realitatea este că o protecție cu vocație universală, bazată pe pârghii juridice și instituționale integrate va fi singura soluție care să permită realizarea obiectivelor propuse într-un mod adecvat.

Internaționalizarea protecției datelor personale este influențată și, totodată, se realizează în cadrul unor sectoare profesionale specifice, cum este situația **sectorului medical și de sănătate**. Privit la modul cel mai umanist posibil, sectorul medical cuprinde imperativele cele mai puternice care generează internaționalizarea, deoarece circulația datelor în acest sector conduce la salvarea de vieți omenești și, la modul general, contribuie la creșterea calității vieții oamenilor. Pornind de la aceste imperative, încă din 2015 Comisia Europeană a lansat programul creării unei Piețe digitale unice, în cadrul agendei sale figurând și sectorul medical.

Privită dintr-o perspectivă juridică, internaționalizarea protecției datelor în sectorul medical și de sănătate se fundamentează pe **modul de interacțiune** dintre sistemele naționale, sistemele regionale de integrare (cum este cazul Uniunii Europene) și sistemul internațional. Acest mod de interacțiune este unul extrem de complex, deoarece presupune o dinamică în sensuri multiple și intervenția unor entități dintre cele mai variate. Există însă, cel puțin în ceea ce privește țările din Uniunea Europeană, repere extrem de clare, fără însă a se exclude o varietate de perspective, deoarece **prima linie de apărare și protecție a drepturilor rămâne întotdeauna cadrul național**.

În cadrul național, eficiența protecției drepturilor și a datelor ar putea să fie cea mai mare, deoarece în acest cadru apare de cele mai multe ori necesitatea îngrijirilor medicale și aici s-ar putea interveni direct cel mai repede. Obligațiile ce însoțesc acordarea diferitelor tratamente, efectuarea diferitelor cercetări sau achiziții tehnologice sunt influențate de cadrul juridic internațional, inclusiv acordarea unor garanții juridice al căror rost este de a proteja dreptul la viață, dreptul la sănătate și viața privată a persoanelor.

În cele ce urmează, prezentăm **algoritmul juridic internațional de bază**, pornind din unghiul dreptului la protecția datelor în domeniul sănătății, astfel cum acesta este ocrotit de legislația europeană.

În Uniunea Europeană avem principii și reglementări fundamentale **interconectate**, a căror aplicabilitate se întinde în realitate la nivelul întregii Europe, doar că diferă modul de protecție și recepționare a lor în dreptul național al statelor europene. Aceste principii și reglementări fundamentale sunt stipulate de **Carta drepturilor fundamentale a Uniunii Europene** (CDFUE) și în **Convenția europeană a drepturilor omului** (CEDO). CDFUE (2000) este actul juridic cu cea mai mare forță juridică, aplicabil la nivelul Uniunii Europene și a statelor membre, iar CEDO (1950) este actul juridic adoptat sub auspiciile Consiliului Europei, aplicabil la nivelul celor 46 de state membre (*până la data de 16 martie 2022, Consiliul Europei avea 47 de state membre, dată de la care Federația Rusă nu mai este stat membru, urmare a retragerii sale în contextul conflictului armat din Ucraina și a evoluțiilor din plan internațional*).

Carta drepturilor fundamentale a Uniunii Europene este elaborată pe baza expertizei și evoluțiilor de mai multe decenii în domeniul de aplicabilitate a CEDO.

CDFUE statuează două drepturi fundamentale care protejează valori pe care se fundamentează juridic protecția datelor cu caracter personal: **articolul 7**, denumit „Respectarea vieții private și de familie” și **articolul 8**, denumit „Protecția datelor cu caracter personal”.

Articolul 7 are următorul conținut:

- *Orice persoană are dreptul la respectarea vieții private și de familie, a domiciliului și a secretului comunicațiilor.*

Articolul 8 stipulează în felul următor:

- *(1) Orice persoană are dreptul la protecția datelor cu caracter personal care o privesc.*
- *(2) Asemenea date trebuie tratate în mod corect, în scopurile precizate și pe baza consimțământului persoanei interesate sau în temeiul unui alt motiv legitim prevăzut de lege. Orice persoană are dreptul de acces la datele colectate care o privesc, precum și dreptul de a obține rectificarea acestora.*
- *(3) Respectarea acestor norme se supune controlului unei autorități independente.*

Cele două articole din CDFUE asigură o protecție juridică mai calitativă decât articolul 8 (Dreptul la respectarea vieții private și de familie) al Convenției europene a drepturilor omului, însă, realitatea este că rolul CEDO se menține la aceleași standarde, deoarece jurisprudența **Curții europene a drepturilor omului (Strasbourg)**, cea care judecă în temeiul **CEDO**, a stat la baza înțelegerii și dezvoltării protecției drepturilor omului în general (implicit și a dreptului la viață privată) și continuă să rămână, fiind încorporată de sistemul de drept al Uniunii Europene sub forma **principiilor generale ale dreptului**.

În mod asemănător, la nivelul Uniunii Europene, jurisprudența dezvoltată de Curtea de Justiție a Uniunii Europene (Luxembourg), furnizează reperele de înțelegere a Cartei drepturilor fundamentale și, totodată, contribuie la formarea și dezvoltarea unor principii generale ale dreptului. Între cele două sisteme, cel al Uniunii Europene și cel al Consiliului Europei, interconectarea juridică se realizează în baza articolului 6 alin. (3) din **Tratatul privind Uniunea Europeană**, care prevede următoarele:

- *(3) Drepturile fundamentale, astfel cum sunt garantate prin Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale și astfel cum rezultă din tradițiile constituționale comune statelor membre, constituie principii generale ale dreptului Uniunii.*

Ca urmare, se poate concluziona că articolul 8 din Convenția europeană a drepturilor omului coroborat cu articolele 7 și 8 din Carta drepturilor fundamentale a Uniunii Europene, reprezintă baza juridică primară pe care se construiesc toate reglementările de protecție a datelor cu caracter personal în UE, inclusiv ceea ce este cunoscut azi sub denumirea Regulamentul General privind Protecția Datelor.

La nivelul Europei, una dintre reglementările internaționale specific dedicate protecției datelor cu caracter personal este **Convenția pentru protecția persoanelor fizice în ceea ce privește prelucrarea automatizată a datelor cu caracter personal (1981), denumită Convenția 108+.** Aceasta reflectă în mare măsură regulile cuprinse de RGPD, deoarece reformarea convenției a fost realizată relativ recent.

Toate aceste reglementări specifice protecției datelor cu caracter personal trebuie privite în **contextul sectorial specific**, adică cel al **sănătății**. Din acest unghi, vom observa că, la nivelul sistemului de drept al UE, protecția datelor interferează foarte mult cu dreptul la demnitate (articolul 1 CDFUE), dreptul la viață (articolul 2 CDFUE), cu dreptul la integritate (articolul 3 CDFUE), iar protecția generală este garantată de articolul 35 CDFUE, denumit **„Protecția sănătății”**, care stabilește următoarele:

- *Orice persoană are dreptul de acces la asistența medicală preventivă și de a beneficia de îngrijiri medicale în condițiile stabilite de legislațiile și practicile naționale. În definirea și punerea în aplicare a tuturor politicilor și acțiunilor Uniunii se asigură un nivel ridicat de protecție a sănătății umane.*

Întrucât cuprinde dispoziții specifice, redăm aici și conținutul articolului 3, denumit **Dreptul la integritate:**

- *(1) Orice persoană are dreptul la integritate fizică și psihică.*
- *(2) În domeniile medicinei și biologiei trebuie respectate în special:*
    - *(a) consimțământul liber și în cunoștință de cauză al persoanei interesate, în conformitate cu procedurile prevăzute de lege;*
    - *(b) interzicerea practicilor de eugenie, în special a celor care au drept scop selecția persoanelor;*
    - *(c) interzicerea utilizării corpului uman și a părților sale, ca atare, ca sursă de profit;*
    - *(d) interzicerea clonării ființelor umane în scopul reproducerii*

În plus, la nivel european este extrem de relevantă Convenția europeană din

4 aprilie 1997 pentru protecția drepturilor omului și a demnității ființei umane față de aplicațiile biologiei și medicinei, Convenția privind drepturile omului și biomedicina*), cunoscută și sub denumirea de **Convenția de la Oviedo**. Acest domeniu reglementat la nivel internațional european, este cunoscut și sub denumirea de bioetică, știință care se preocupă de **implicațiile progresului din biomedicină**, datorat mai ales dezvoltării tehnologice, asupra **ființei umane,** la nivelul **drepturilor omului** și al demnității umane. Iată câteva dintre problematicile specifice bioeticii:

- Procrearea medicală asistată
- Consimțământul pentru intervenția medicală
- Stocarea informațiilor biologice pentru cercetare
- Prelucrarea datelor privind Testarea genetică și rezultatele diferitelor analize
- Utilizarea informațiilor medicale în scopuri comerciale și de asigurare
- Donarea de organe de către vii

Dezvoltarea științelor biomedicale presupune provocări juridice, în special care țin de drepturile omului, precum dreptul la integritate fizică și la viață, dreptul la demnitate, dreptul la viață privată și la protecția datelor, dreptul la un nivel de trai decent. Ca urmare, una dintre cauzele internaționalizării protecției datelor cu caracter personal este **dezvoltarea tehnologiei și progresul științific**.

Convenția de la Oviedo reprezintă **instrumentul recent, modern și specific**, alături de 4 protocoale adiționale la Convenție, menit să protejeze drepturile omului și demnitatea umană în cadrul sferei biomedicinei. Convenția este ratificată de România prin **Legea nr. 17/2001 privind ratificarea** Convenției europene pentru protecția drepturilor omului și a demnității ființei umane față de **aplicațiile biologiei și medicinei**, Convenția privind drepturile omului și biomedicina, semnată la Oviedo la 4 aprilie 1997, și a Protocolului adițional la Convenția europeană pentru protecția drepturilor omului și a demnității ființei umane față de aplicațiile biologiei și medicinei, referitor la **interzicerea clonării ființelor umane**, semnat la Paris la 12 ianuarie 1998. Convenția stabilește **obligații pentru statele membre**, cum ar fi:

- să pună la dispoziția celor interesați o **procedură judiciară** rapidă și adecvată, capabilă să prevină sau să pună capăt, în cel mai scurt timp, unei încălcări ilegale sau unei amenințări la adresa principiilor (articolul 23)
- să creeze un sistem prin care cei care au avut de suferit vătămări nejustificate ca urmare a unei intervenții medicale, să beneficieze de o **compensație echitabilă** (articolul 24)

La nivelul Consiliului Europei trebuie avute în vedere acele acte juridice internaționale și acele îndrumări care sunt specifice sectorului medical sau bioeticii. Prin intermediul acestora se poate, într-un anumit cadru, face aplicarea mai în detaliu a principiilor de protecție a datelor, inclusiv a principiilor etice.

Principalele instrumente în domeniul bioeticii, al sănătății și al protecției datelor. Cadrul juridic internațional.

- 1950 - Convenția europeană a drepturilor omului
- 1981 - Convenția pentru protecția persoanelor fizice în ceea ce privește prelucrarea automatizată a datelor cu caracter personal, reformată în 2018 și denumită Convenția 108+
- 1997 - Convenția de la Oviedo pentru protecția drepturilor omului și a demnității umane față de aplicațiile biologiei și medicinei
- 1998 - Protocolul adițional la Convenția de la Oviedo, privind interzicerea clonării ființelor umane
- 2000 - Carta Drepturilor Fundamentale a Uniunii Europene
- 2002 - Protocolul adițional la Convenția de la Oviedo, privind transplantul organelor și al țesuturilor de origine umană
- 2005 - Protocolul adițional la Convenția de la Oviedo, privind cercetarea biomedicală
- 2008 - Protocolul adițional la Convenția de la Oviedo, privind testarea genetică în scopuri de sănătate

Alte instrumente internaționale:

- 2003 - Rec(2003)10 a Comitetului de Miniștri privind xenotransplantarea și Memorandumul explicativ
- 2004 - Rec(2004)10 a Comitetului de Miniștri cu privire la protecția drepturilor omului și a demnității persoanelor cu dizabilitate mintală și memorandumul explicativ
- 2006 - Rec(2006)4 a Comitetului de Miniștri cu privire la cercetarea materialelor biologice și originea umană
- 2016 - Rec(2016)6 a Comitetului de Miniștri către Statele Membre cu privire la cercetarea materialelor biologice de origine umană
- 2016 - Rec(2016)8 a Comitetului de Miniștri cu privire la prelucrarea datelor personale privind sănătatea pentru scopuri de asigurări, inclusiv datele rezultate din teste genetice și Memorandumul explicativ
- 2019 - Rec(2019)2 a Comitetului de Miniștri privind protecția datelor medicale

Instrumente internaționale de recomandare:

- 1997 - Declarația Universală cu privire la genomul uman și drepturile omului
- 2003 - Declarația Internațională cu privire la datele genetice umane
- 2005 - Declarația Universală cu privire la bioetica și drepturile omului

Protecția garantată de Convenția europeană a drepturilor omului și jurisprudența Curții europene a drepturilor omului

Valențele unor drepturi garantate de CEDO se răsfrâng și asupra activităților biomedicale, deoarece în esență asemenea activități au ca obiect material ființa biologică, fizică și psihică. Tradițional sunt puse în discuție trei drepturi:

- Dreptul la viață (articolul 2)
- Dreptul de a nu fi supus torturii, tratamentelor inumane și degradante (articolul 3)
- Dreptul la viață privată (articolul 8)

În plus, jurisprudența este un instrument în sine, distinct, de care trebuie să ținem cont, deoarece lămurește problematica protecției datelor pe situații concrete, oferind avantajul de a crea tipare utile în activitățile curente, deoarece permit identificarea rapidă a modelului de urmat sau de înlăturat.

Exemple din jurisprudența Curții europene privind bioetica și protecția datelor medicale

- *Pretty împotriva Regatului Unit* - cauza în care Curtea europeană a stabilit că dreptul la viață **nu** presupune **dreptul de a muri**.
- *Aleksanyan împotriva Rusiei* - cauza care pune în discuție **absența asistenței medicale** pentru un bolnav diagnosticat HIV pozitiv și aflat în detenție. Curtea europeană a stabilit că netransferarea deținutului către un spital extern cu capabilități adecvate i-a lezat demnitatea și i-a cauzat complicații acute, sporind gradul de suferință cauzat de bolile de care suferea și de condamnarea la închisoare, astfel încât s-a considerat că Rusia se face vinovată de **tratamente inumane și degradante**, încălcând articolul 3 din Convenția europeană.

- *Glass împotriva Regatului Unit* - aduce în discuție **administrarea unui tratament medicamentos** (diamorfină) pentru a ușura suferința unui copil aflat în fază terminală, **fără a exista acordul mamei** și fără a exista o autorizație din partea unei instanțe de judecată. Curtea a apreciat că a fost încălcat articolul 8 din Convenție **(viața privată).**
- *L.H. împotriva Letoniei* - reclamanta a pretins în special că **colectarea datelor sale medicale** personale de către o agenție de stat - în acest caz, Inspectoratul pentru controlul calității asistenței medicale și a aptitudinii pentru muncă ("MADEKKI") - **fără consimțământul său**, i-a încălcat dreptul la respectarea vieții sale private. În această hotărâre, Curtea a reamintit importanța protecției datelor medicale pentru ca o persoană să se bucure de dreptul la respectarea vieții private. Aceasta a considerat că a existat o încălcare a articolului 8 din Convenție în cazul reclamantei, constatând că legea aplicabilă nu a indicat cu suficientă claritate domeniul de aplicare a puterii de apreciere conferită autorităților competente și modul de exercitare a acesteia. Curtea a remarcat în special că legislația letonă nu a limitat în niciun fel domeniul de aplicare a datelor cu caracter privat care ar putea fi colectate de MADEKKI, ceea ce a dus la colectarea de către aceasta a datelor medicale ale reclamantei referitoare la o perioadă de șapte ani, fără discernământ și fără nicio evaluare prealabilă dacă astfel de date ar putea fi potențial decisive, relevante sau importante pentru a realiza orice scop care ar fi putut fi urmărit prin ancheta în cauză.

Tendințele din Uniunea Europeană privind datele medicale

În primul rând, așa cum am menționat în partea de început a acestui curs, Uniunea Europeană are printre obiective **digitalizarea sectorului medical**. Piața digitală unică (DSM - digital single market) urmărește să aducă oportunitățile digitale la un nivel strategic al pieței. În această idee Comunicarea Comisiei Europene privind Transformarea digitală a sectorului medical și de asistență în Piața digitală unică, evidențiază trei aspecte prioritare:

- Accesul în siguranță al cetățenilor la datele medicale proprii, inclusiv transfrontalier
- Servicii medicale personalizate prin infrastructura de date comună europeană
- Crearea de instrumente digitale pentru a se trimite reacțiile utilizatorilor și îngrijirea centrată pe persoană

În raportul asupra **dosarului electronic medical**, realizat de grupul de experți în protecția datelor, se face o interpretare a principiilor de protecție a datelor la sistemele electronice de dosare medicale și sunt propuse o serie de **garanții** legale pentru protejarea confidențialității medicale a persoanei. Grupul de experți definește dosarul electronic medical ca fiind un dosar medical complet sau documentația similară privind starea de sănătate fizică sau mentală, trecută și prezentă unui a unui individ, în formă electronică și care asigură disponibilitatea ușor accesibilă a acestor date pentru tratatement medical sau alte scopuri strâns legate de acesta.

Interoperabilitatea sistemelor de evidență este un obiectiv distinct și apare afirmat în Recomandarea Comisiei Europene, din 2 iulie 2008, privind interoperabilitatea transfrontalieră a sistemelor de evidență electronică a datelor medicale. În cadrul Recomandării se propune stabilirea unui cadru juridic adecvat, necesar protecției vieții private în mediul electronic.

Asistența medicală transfrontalieră este reglementată de Directiva 2011/24/EU a Parlamentului european și a Consiliului din 9 martie 2011 privind aplicarea drepturilor pacienților în cadrul asistenței medicale transfrontaliere. Directiva stabilește drepturile pacienților să solicite servicii medicale în altă țară europeană și să solicite rambursarea și creează baza pentru schimbul transfrontalier de date medicale. Directiva stabilește crearea rețelei voluntare de autorități naționale responsabile cu eHealth, care susțin cooperarea dintre statele membre. Ulterior, rețeaua a formulat instrucțiunile necesare pentru rețete medicale electronice care să poată fi recepționate transfrontalier, asigurându-se interoperabilitatea lor.

E-Sănătatea reprezintă o linie strategică în Uniunea Europeană. E-Sănătatea este obiectivul care presupune împuternicirea pacienților, medicilor și personalului medical de a recurge la conectarea de dispozitive și tehnologii și de a investi în cercetări care să conducă la medicina personalizată a viitorului. Rezultatul va fi asigurarea unor servicii medicale mai inteligente, mai sigure și centrate pe pacient.

În continuare vom reda expunerea de motive la raportul Parlamentului European referitor la Planul de acțiune privind e-Sănătatea 2012-2020: asistență medicală inovatoare pentru secolul XXI:

- „E-sănătatea reprezintă o modalitate de îmbunătățire a calității și eficienței asistenței medicale în secolul XXI și de a asigura accesul universal la aceasta.

- Piața potențială a e-sănătății este solidă. Astfel, piața mondială a telemedicinei a ajuns de la 9 800 de milioane de dolari în 2010, la 11 600 de milioane de dolari în 2011, estimându-se că va continua să se dezvolte, ajungând la 27 300 de milioane de dolari în 2016, rata medie de creștere anuală fiind de 18,6 %.

- În pofida faptului că accesul la asistență medicală de calitate este un drept fundamental recunoscut, creșterea cererii de servicii medicale ca urmare a **îmbătrânirii populației**, a impactului bolilor cronice, a mobilității pacienților și specialiștilor în domeniul medical, precum și așteptările mai ridicate ale cetățenilor în ceea ce privește calitatea asistenței medicale și bugetele din ce în ce mai limitate în domeniul medical au creat numeroase probleme, cu care se confruntă în prezent sistemele de sănătate din întreaga UE.

- E-Sănătatea poate contribui la realizarea acestor obiective, întrucât contribuie la îmbunătățirea accesului la servicii de sănătate pentru persoanele care trăiesc în regiuni îndepărtate și slab populate, la îmbunătățirea condițiilor de muncă, la reducerea timpului de așteptare, precum și, mai presus de toate, la asigurarea furnizării de asistență medicală de încredere, eficientă și de înaltă calitate.

- Cu toate acestea, pentru a realiza aceste obiective, este necesar ca furnizorii de servicii de sănătate să colaboreze între ei, nu numai în domeniile lor de competență ci și dincolo de barierele lingvistice, pentru a oferi servicii de calitate care vizează îndeosebi siguranța pacienților. În acest sens, este necesar să se instituie standarde tehnice, să se asigure interoperabilitatea sistemelor de sănătate europene și să se stabilească scheme de certificare și autentificare la nivelul UE.

- Pentru ca atât cetățenii, cât și specialiștii din domeniul sănătății să aibă încredere în beneficiile aplicațiilor de e-sănătate, acestea trebuie să beneficieze de securitate juridică. Protecția datelor, confidențialitatea, viața privată și responsabilitatea sunt unele dintre chestiunile care trebuie rezolvate pentru ca aplicarea serviciilor de e-sănătate să fie o reușită.

- Este esențial ca statele membre să facă schimb de experiență, cunoștințe și bune practici, colaborând între ele și cu Comisia pentru a îmbunătăți, astfel, sistemele de e-sănătate. Este de dorit ca, în viitor, e-Sănătatea să devină o realitate și, la realizarea acestui obiectiv, pot contribui statele membre care sunt pionieri în domeniu, împărtășind cunoștințele lor cu cele care nu sunt.

- Este esențial ca, la dezvoltarea aplicațiilor de e-sănătate și după aceea, să se țină seama atât de punctul de vedere al medicilor și al specialiștilor în domeniul sănătății, cât și de cel al asociațiilor de pacienți. Ei sunt cei ce le vor utiliza și, de aceea, trebuie să fie convinși de utilitatea lor și să știe să le folosească; astfel, atât sectorul public, cât și cel privat trebuie să ofere toate informațiile necesare, într-o manieră clară și adaptată sectorului căruia i se adresează.

- Nu în ultimul rând, este esențial ca, la dezvoltarea acestor proiecte, să se aibă în vedere în mod prioritar interesul pacienților, întrucât, la urma urmei, obiectivul nostru principal este îmbunătățirea calității asistenței medicale oferite cetățenilor UE, fără a pierde din vedere diferențele culturale dintre statele membre ale UE în domeniul asistenței medicale.

4.3 PRINCIPIILE PROTECȚIEI DATELOR

- Cunoașterea întregului corpus de principii ale prelucrării datelor medicale
- Înțelegerea modalității de aplicare generală a acestor principii
- Prezentarea normelor juridice de referință

Modalitatea de realizare a secțiunii:

În partea teoretică a ghidului dorința a fost să se creeze un interes și o conștientizare că activitatea medicală se bazează pe standarde juridice și etice încorporate organic prin intermediul unui mecanism exterior esenței activității medicale: protecția datelor cu caracter personal.

În această parte a ghidului se impune aprofundarea, în sensul precizării stricte a principiilor în materia protecției datelor cu caracter personal, așa cum acestea figurează în legislația de protecție a datelor. Ca urmare, această parte va avea un caracter și mai accentuat juridic. Din acest motiv, pentru a fi cât mai firesc înțelese, principiile sunt însoțite în mod constant de exemple care nu sunt neapărat prezentate în limbaj juridic, dar sunt realizate după o formulă logică, comună inclusiv domeniului juridic.

Am considerat util să se facă trimitere strict la o legislație corespunzătoare, însă aceste referiri trebuie înțelese doar ca un instrument doveditor al principiilor expuse, util în special atunci când este confruntat cineva cu suportul legal al problematicilor de protecție a datelor medicale.

Referitor la legislația de protecție a datelor, ghidul în mod intenționat nu urmărește să dezvolte problematici extrem de specifice domeniului juridic, cum ar fi relația dintre normele internaționale, normele Uniunii Europene și legislația națională; principii de interpretare a normelor juridice; rolul precedentelor judiciare asupra înțelegerii principiilor etc. Am considerat că acest ghid are ca adresabilitate în special practicienii și profesioniștii din sistemul medical și din sănătate, astfel că o consultanță strictă de specialitate în domeniul protecției datelor trebuie obținută prin a apela la specialiști.

Scopul principal al ghidului este orientarea și încorporarea conștientă a standardului de protecție a datelor în activitatea medicală, astfel încât să fie obținute rezultate, precum: **îmbunătățirea cunoștințelor, abilităților și performanțelor în activitatea medicală**; îmbunătățirea și garantarea **securității și calității profesiei și activității medicale**; creșterea nivelului de **comunicare, de cooperare și de lucru în echipă**; menținerea **încrederii în activitatea medicală și în profesioniștii din sectorul medical**, atât din partea publicului larg cât și în special în relația dintre medic și pacient.

Din perspectiva protecției datelor personale, una dintre consecințele parcurgerii ghidului este ridicarea progresivă dar constantă a conformității cu Regulamentul General privind Protecția Datelor, deoarece acesta stabilește implicit obligația de instruire pentru operatorii de date (ex. unități medicale - spitale, clinici, cabinete medicale).

Principiile de prelucrare a datelor medicale

I. **Un prim mod de abordare a datelor medicale** este acela care ia în considerare **contactul direct** cu acestea și **maniera** în care trebuie ele **prelucrate**. De aceea, într-o activitate medicală, trebuie să identificăm persoanele implicate în colectarea datelor, organizarea lor, valorificarea lor prin toate modalitățile. Medicul rămâne principalul personaj care generează și fructifică aceste date, însă activitatea presupune intervenția multor altor persoane, precum asistenți medicali, personal administrativ etc. **Răspunderea pentru aceste date revine operatorului de date (spitalului, cabinetului medical sau oricărei alte forme juridice de organizare a activității), însă persoanele fizice care lucrează cu aceste date în mod direct și palpabil trebuie să cunoască bine regulile de urmat pentru prelucrarea datelor cu caracter medical**. Primul principiu a fost dezvoltat și în partea introductivă a ghidului, însă aici este reluat în contextul „arhitecturii" de ansamblu a principiilor de protecție a datelor.

Orice persoană care prelucrează date referitoare la sănătate trebuie să respecte următoarele **principii**:

DATELE TREBUIE SĂ FIE PRELUCRATE ÎNTR-UN MOD TRANSPARENT, LEGAL ȘI ECHITABIL

Respectarea acestui principiu va asigura medicului stabilirea unei relații de încredere cu pacientul, va asigura calitatea și securitatea datelor medicale și va conduce la rezultate medicale de calitate.

Texte legale aplicabile: RGPD impune respectarea și aplicabilitatea acestui principiu la articolul 5 alin. 1 lit. a), dar el este precizat în mod specific în numeroase secvențe și ipoteze avute în vedere de legislația națională, în special de **Legea 95/2006 privind reforma în domeniul sănătății, republicată**.
Astfel vorbim despre:

- **Articolul 30^8 al legii 95/2006** stabilește obligația generală de prelucrare a datelor în conformitate cu prevederile legale, obligație care aparține cabinetelor medicale ambulatorii ale medicilor de familie şi de alte specialități, centre de diagnostic și tratament, centre medicale, centre de sănătate, laboratoare, precum și prin alte unități sanitare publice și private, unităților sanitare publice şi private cu paturi.

- **Articolul 40 al Legii 95/2006** stabilește temeiul legal al unei situații specifice de prelucrare, precum aceea de păstrare a datelor privind sănătatea de către autoritățile de sănătate publică, cu scopul întocmirii de statistici și limitează utilizarea lor pentru alte scopuri, dacă nu există o dispoziție legală în acest sens, consimțământul persoanei vizate, protejarea unui interes vital sau a unui interes public major, ori necesitatea efectuării urmăririi penale.

- **Articolul 108 al Legii 95/2006** are în vedere stabilirea regulilor de înființare și organizare a spitalelor de urgență, context în care stabilește norma de organizare pe linia de colectare a datelor, precizând explicit că modalitățile de colectare se vor stabili cu respectarea prevederilor legale în vigoare privind protecția datelor cu caracter personal.

- **Articolul 138 al Legii 95/2006** impune obligații specifice furnizorilor de servicii medicale de specialitate în ceea ce privește utilizarea datelor colectate rezultate din activitatea proprie, raportările de date către autoritățile publice și arhivarea acestora, conform prevederilor legale.

- **Articolul 145 al Legii 95/2006** stabilește interdicția generală de prelevare de organe, ţesuturi şi celule de la potenţiali donatori minori în viaţă, cu excepţia cazurilor prevăzute de această lege, stabilind garanții specifice acestei situații, garanții situate la nivelul consimțământului minorilor.

- **Articolul 346^5 al Legii 95/2006** referitor la DES, stabilește regula că Prelucrarea datelor cu caracter personal în cadrul DES, ca parte componentă a Platformei informatice din asigurările de sănătate, se realizează cu respectarea prevederilor Regulamentului General privind Protecția Datelor.

- **Articolul 346^6 al Legii 95/2006** cuprinde reguli privind conținutul dosarului medical și condițiile de accesare a acestuia, în special privind echitatea procedurilor bazate pe consimțământul pacientului.

- **Articolele 346^7, 346^8, 346^9 ale Legii 95/2006** stabilesc o serie de reguli privind accesul la datele și informațiile din DES, cazuri de acces fără a fi necesar consimțământul persoanei vizate și unele concepte specifice DES. Toate acestea sunt condiționate de respectarea prevederilor RGPD.

- **Articolul 346^11 al Legii 95/2006** ne indică concret **obligația medicilor** de a respecta principiile de deontologie și etică medicală, cu respectarea legii și a normelor de protecție a datelor cu caracter personal, ori de câte ori utilizează DES al pacienților. Totodată, se impune obligația asigurării dreptului la informare și a tuturor drepturilor specifice pacienților.

- **Articolele 661 și 662 ale Legii 95/2006** stabilesc condițiile pentru exprimarea **consimțământului informat**, inclusiv situațiile de excepție și răspunderile aferente medicilor, asistenților medicali sau moașelor pentru nerespectarea prevederilor privind consimțământul informat.

- **Articolul 696 al Legii 95/2006** evidențiază un **caz distinct de prelucrare a datelor medicale**, motivat de **scopul analizelor și monitorizării serviciilor de sănătate** decontate din fondul de asigurări de sănătate. Instituția abilitată prin lege pentru colectarea datelor și prelucrarea lor în scopurile menționate este **INMSS**.

- **Articolul 910 al Legii 95/2006** stabilește **principalele obligații de informare a pacienților de către furnizorii de servicii medicale**, informații necesare pentru asigurarea consimțământului informat, asigurarea căilor de recuperare a unor prejudicii de către pacienți, să asigure nediscriminatoriu asistență medicală, inclusiv transfrontalieră și să respecte confidențialitatea datelor cu caracter personal în conformitate cu prevederile legale în materie.

- **Legea drepturilor pacientului nr. 46/2003** Contractul Cadru și Normele de aplicare ale COCA – pentru contractele realizate de furnizorii de servicii medicale – medicină de familie, ambulatoriu de specialitate, spitale, farmacii, îngrijiri la domiciliu și îngrijiri paliative.

Exemplu de bună practică în respectarea principiului legalității, echității și transparenței prelucrării datelor medicale de către un medic:

- Un medic solicită în mod explicit consimțământul pacienților înainte de a utiliza datele lor medicale într-un studiu științific. Medicul ar trebui să informeze pacienții despre **scopul studiului, modul în care vor fi utilizate datele lor personale, drepturile lor de acces, rectificare și ștergere a datelor** și să le ofere opțiunea de a se retrage din studiu în orice moment.

Exemplu din cazuistică

Autoritatea Națională de Supraveghere (A.N.S.) din România a finalizat în luna decembrie 2022 două investigații la un cabinet stomatologic și la un medic stomatolog (colaborator al cabinetului stomatologic) ambii operatori de date cu caracter personal.

În cadrul investigațiilor efectuate, s-a constatat că operatorii au divulgat informații medicale referitoare la tratamentul ortodontic al petiționarului Autorității (A.N.S.), constând într-un set de fotografii și radiografii care se puteau corela cu numele persoanei, prin publicarea unui articol pe un blog de specialitate. Aceste informații au fost publicate atât în scop științific, cât și în scop comercial.

A.N.S. a aplicat cabinetului stomatologic sancțiunea contravențională a amenzii în cuantum de 4.919,2 lei pentru încălcarea articolului 33 din RGPD și a aplicat medicului stomatolog colaborator sancțiunea contravențională a amenzii în cuantum de 4.919,2 lei pentru încălcarea dispozițiilor art. 6 alin. (1) lit. a) și ale art. 9 alin. (2) lit. a) din RGPD. Principala fundamentare a aplicării amenzii a fost că operatorul medic stomatolog colaborator a prelucrat, inclusiv prin utilizare și dezvăluire, datele personale privind starea de sănătate a persoanei vizate, în cadrul unui articol postat pe blogul personal, **fără să prezinte dovezi privind obținerea consimțământului expres al persoanei implicate și fără informarea sa prealabilă.**

Acest exemplu evidențiază încălcarea atât a principiului legalității cât și a echității prelucrării datelor medicale ale pacienților.

Pentru a ilustra pe larg diverse situații relevante specifice acestui principiu, vă rugăm să parcurgeți:

- **Orientarea 3.10** cu privire la **gestionarea cererilor persoanelor vizate** (pacienți / aparținători) cu privire la propriile informații
- **Orientarea 3.8** cu privire **la protejarea datelor în afara cadrului profesional** de desfășurare a activității

DATELE TREBUIE COLECTATE ÎN SCOPURI DETERMINATE, EXPLICITE ȘI LEGITIME ȘI NU TREBUIE PRELUCRATE ULTERIOR ÎNTR-UN MOD INCOMPATIBIL CU ACESTE SCOPURI

PRELUCRAREA ULTERIOARĂ ÎN SCOPURI DE ARHIVARE ÎN INTERES PUBLIC, ÎN SCOPURI DE CERCETARE ȘTIINȚIFICĂ SAU ISTORICĂ ORI ÎN SCOPURI STATISTICE NU ESTE CONSIDERATĂ INCOMPATIBILĂ CU SCOPURILE INIȚIALE, DAR TREBUIE SĂ EXISTE GARANȚII PENTRU RESPECTAREA DREPTURILOR ȘI LIBERTĂȚILOR PERSOANELOR

Texte legale aplicabile: RGPD impune respectarea și aplicabilitatea acestui principiu la articolul 5 alin. 1 lit. b), dar și acesta este precizat în mod specific în numeroase secvențe și ipoteze avute în vedere de legislația națională, în special de **Legea 95/2006 privind reforma în domeniul sănătății, republicată.**

Unul dintre exemplele ilustrative este reglementat de articolul 346^12 al Legii 95/2006 și se referă la **refuzul expres al pacienților de a li se utiliza dosarul electronic de sănătate**, precum și la utilizarea datelor din DES în scopuri de arhivare în interes public, cercetare științifică și scopuri statistice. Potrivit acestui articol pacienții care în mod expres refuză să accepte utilizarea DES, datele acestora nu vor putea fi introduse în DES, iar cele deja introduse pot fi complet anonimizate dacă pacientul solicită acest lucru, ceea ce înseamnă că nu vor mai putea fi corelate electronic cu identitatea pacientului. Această situație, chiar reglementată, evidențiază că natura sensibilă a datelor medicale justifică necesitatea ca datele să fie anonimizate dacă au fost introduse în DES, deoarece altfel principiul legitimității scopurilor prelucrării datelor nu ar fi respectat, deoarece **acordarea îngrijirilor medicale nu poate fi condiționată de „acordul" pacientului de a i se utiliza datele din DES**.

Exemplu de bună practică

- O bună practică în colectarea datelor personale în activitatea medicală ar putea fi ***utilizarea unui sistem de management al pacienților*** într-un spital. În acest context, scopurile determinate, explicite și legitime ale colectării datelor personale ale pacienților ar putea include:
    - Îmbunătățirea calității îngrijirii medicale oferite pacienților
    - Monitorizarea și prevenirea potențialelor riscuri și incidente în domeniul sănătății
    - Ușurarea comunicării între personalul medical și pacienți
    - Managementul eficient al resurselor spitalicești

Astfel, datele personale colectate ar trebui să fie limitate la informațiile necesare pentru atingerea acestor scopuri, precum numele, adresa, numărul de telefon, data nașterii, istoricul medical și diagnosticul. Datele nu ar trebui să fie prelucrate în moduri care nu sunt compatibile cu aceste scopuri, cum ar fi comercializarea sau utilizarea acestora în cercetări care nu sunt legate de îmbunătățirea sănătății pacienților.

Cu toate acestea, măsurile de siguranță ar trebui să fie sporite, informarea pacienților trebuie să fie extrem de completă și transparentă, iar după atingerea acestui scop principal, acela al îngrijirilor medicale spre exemplu, informațiile ar trebui anonimizate în cel mai scurt timp.

Exemplu din cazuistică

În cauza denumită Lindqvist (C-101/01), Curtea de Justiție a Uniunii Europene (CJUE) a examinat problematica publicării pe internet de către o persoană a unor date personale despre colegii săi dintr-o asociație cu caracter religios, inclusiv informații despre starea lor de sănătate. Aceste informații au putut fi accesate prin intermediul unei pagini web, deși la momentul colectării acestora scopul era exclusiv în interesul funcționării acelei asociații, iar membrii asociației nici nu fuseseră informați nici nu li se ceruse consimțământul pentru publicarea respectivelor date. Practic, scopul publicării pe site-ul web nu mai era compatibil cu scopul inițial pentru care datele au fost colectate. Curtea a constatat că publicarea informațiilor a încălcat principiul ca datele personale să fie colectate și prelucrate numai în scopuri determinate, explicite și legitime, conform Directivei 95/46/CE privind protecția datelor personale, care a fost înlocuită ulterior de Regulamentul General privind Protecția Datelor (GDPR).

O altă situație de încălcare a principiului colectării datelor a fost supusă investigației Autorității Naționale de Supraveghere, care a aplicat o amendă de aproximativ 2000 Euro unui centru medical, în luna noiembrie 2021 deoarece a dezvăluit date ale unui fost pacient unui alt operator, fără a-l informa sau a-i cere consimțământul.

Pentru a ilustra pe larg diverse situații relevante specifice acestui principiu, vă rugăm să parcurgeți:

- **Orientarea 3.5** cu privire la **posibilitatea de fotografiere, realizarea de capturi video și alte imagini folosite în serviciul medical**

PRELUCRAREA DATELOR AR TREBUI SĂ FIE NECESARĂ ȘI PROPORȚIONALĂ ÎN RAPORT CU SCOPUL LEGITIM URMĂRIT ȘI AR TREBUI SĂ FIE EFECTUATĂ NUMAI PE BAZA CONSIMȚĂMÂNTULUI PERSOANEI VIZATE SAU PE UN ALT TEMEI LEGITIM

Texte legale aplicabile: RGPD impune respectarea și aplicabilitatea acestui principiu la articolul 5 alin. 1 lit. c) coroborat cu articolul 9, dar acesta este precizat în mod specific și în numeroase secvențe și ipoteze avute în vedere de legislația națională, în special de **Legea 95/2006 privind reforma în domeniul sănătății, republicată**. Astfel, vorbim despre:

- **Articolul 30^9 al Legii 95/2006** reglementează relația dintre ipoteza telemedicinei și drepturile pacientului, impunând garanții de informare a acestuia asupra a serviciilor disponibile, calității actului medical în contextul mijloacelor tehnice utilizate pentru transmisia de date, necesitatea garantării consimțământului liber și informat al pacientului. Pentru mai multe detalii, a se vedea **Orientarea 3.9** cu privire la **oferirea de servicii de telemedicină**

- **Articolul 101 al Legii 95/2006** reglementează asigurarea asistenței medicale private de urgență, pe baza consimțământului beneficiarului, chiar și atunci când aceasta se acordă pe baza unui contract cu asigurătorul privat.

- **Articolele 144 - 154 ale Legii 95/2006** stabilesc garanții specifice privind donarea de organe, țesuturi și celule de origine animală, astfel încât să fie asigurat consimțământul informat și liber al donatorului, demonstrarea și asigurarea legalității întregii proceduri. Sunt menționate inclusiv condițiile de prelevare de la persoane decedate.

- **Articolul 230 al Legii 95/2006** reglementează relația dintre asigurați, pe de o parte și asigurători și furnizorii de servicii medicale pe de altă parte. Printre drepturile asiguraților se numără și dreptul de a li se garanta confidenţialitatea privind datele, în special în ceea ce priveşte diagnosticul şi tratamentul, precum și dreptul la informaţie în cazul tratamentelor medicale.

- **Articolele 346^1 și următoarele ale Legii 95/2006** reglementează dosarul electronic de sănătate al pacientului, stabilind că acesta conține date și informații clinice, biologice, diagnostice şi terapeutice, personalizate, acumulate pe tot parcursul vieții pacienților. Se stabilesc situațiile de prelucrare electronică a datelor, când nu este necesar consimțământul pacientului, cum este cazul etapei de constituire a acestuia declarându-se activitate de utilitate publică de interes național, precum și situațiile de utilizare a datelor, bazate pe consimțământul pacientului. Sunt stabilite în detaliu categoriile de date prelucrate, procedurile de prelucrare, răspunderea pentru securitatea și încărcarea datelor în DES.

- **Articolele 653 și următoarele ale Legii 95/2006** reglementează problematica răspunderii civile a personalului medical, a psihologilor şi a furnizorilor de servicii conexe actului medical acordate persoanelor diagnosticate cu tulburări din spectrul autist în cadrul programelor naționale de sănătate curative, în toate cazurile această răspundere angajându-se atunci când nu s-au respectat condițiile prevăzute de lege pentru un consimțământ informat, dacă nu ne găsim în situația unor excepții în care consimțământul trebuie acordat de reprezentanții legali ai pacientului.

- Potrivit **articolului 661 al Legii 95/2006** vârsta legală pentru exprimarea consimțământului informat este de 18 ani. Minorii își pot exprima consimțământul în absența părinților sau reprezentantului legal, în următoarele cazuri:
    - situaţii de urgenţă, când părinţii sau reprezentantul legal nu pot fi contactaţi, iar minorul are discernământul necesar pentru a înţelege situaţia medicală în care se află
    - situaţii medicale legate de diagnosticul şi/sau tratamentul problemelor sexuale şi reproductive, la solicitarea expresă a minorului în vârstă de peste 16 ani.

În vederea obţinerii acordului scris al pacientului / reprezentantului legal al acestuia, după caz, psihologul are obligaţia să prezinte pacientului / reprezentantului legal al acestuia informaţii la un nivel ştiinţific rezonabil pentru puterea de înţelegere a acestuia.

Informaţiile trebuie să conţină: metodele utilizate, riscuri, alternative, modul de desfăşurare, frecvenţa, modul în care se poate retrage consimţământul dacă se doreşte acest lucru, limitele confidenţialităţii, inclusiv date privind posibilitatea înregistrării audio-video.

Exprimarea acordului informat este condiţionată de existenţa capacităţii depline de exerciţiu a persoanei cu tulburări din spectrul autist. Modelul de formular pentru consimțământ este stabilit prin Ordin al Ministrul Sănătății, tocmai pentru a garanta în mod specific nivelul de obligativitate și natura sensibilă a datelor medicale.

Exemplu de bună practică privind respectarea principiului prelucrării datelor medicale pe baza consimțământului informat, liber și demonstrabil

Spitalul X implementează un sistem de management al informațiilor medicale pentru a îmbunătăți calitatea serviciilor medicale și a eficientiza procesele interne. Înainte de a prelucra datele medicale ale pacienților, spitalul obține consimțământul scris al pacienților sau al reprezentanților legali ai acestora, în care sunt incluse informații detaliate despre scopul prelucrării datelor, drepturile persoanelor vizate și modalitățile de exercitare a acestor drepturi.

Spitalul limitează accesul la datele medicale doar personalului autorizat și prelucrează datele numai în măsura în care este necesar pentru scopurile medicale stabilite. De asemenea, spitalul implementează măsuri de securitate adecvate pentru a proteja datele pacienților de accesul neautorizat, pierdere sau distrugere.

Cazuistică în domeniu

Un caz notabil în care prelucrarea datelor medicale a fost realizată într-un mod care nu respecta consimțământul pacientului și a fost investigat de Information Commissioner's Office (ICO) din UK. Acest caz implică Royal Free NHS Foundation Trust și DeepMind, o companie de AI deținută de Alphabet, corporația-mamă a Google.

În 2015, **Royal Free NHS Foundation Trust** a încheiat un parteneriat cu **DeepMind** pentru a dezvolta o aplicație numită Streams, care avea ca scop să îmbunătățească tratamentul pacienților cu insuficiență renală acută.

În procesul de a dezvolta această aplicație, Royal Free a oferit DeepMind acces la datele medicale a aproximativ 1,6 milioane de pacienți fără a obține consimțământul explicit al acestora.

În 2017, ICO a finalizat o investigație asupra acestei colaborări și a concluzionat că transferul de date între Royal Free și DeepMind nu respecta legea privind protecția datelor din Marea Britanie. ICO a criticat Royal Free pentru lipsa de transparență și pentru că nu a informat corespunzător pacienții despre cum vor fi utilizate datele lor. Royal Free a fost obligat să efectueze modificări semnificative în ceea ce privește prelucrarea datelor și să își îmbunătățească practicile de protecție a datelor.

În urma acestui caz, DeepMind și Royal Free au luat măsuri pentru a se conforma recomandărilor ICO și a asigura protecția datelor pacienților. Acest caz a servit drept exemplu pentru organizațiile din domeniul sănătății și al tehnologiei în ceea ce privește importanța respectării legilor privind protecția datelor și obținerea consimțământului pacienților înainte de a utiliza datele lor în proiecte similare.

Pentru a ilustra pe larg diverse situații relevante specifice acestui principiu, vă rugăm să parcurgeți:

- **Orientarea 3.13** privitoare la **utilizarea datelor cu caracter personal în scopuri secundare decât cele în care au fost colectate inițial**
- **Orientarea 3.16** privind **obținerea și gestionarea consimțământului persoanei vizate**

DATELE CU CARACTER PERSONAL AR TREBUI, ÎN PRINCIPIU ȘI ÎN MĂSURA ÎN CARE ESTE POSIBIL, SĂ FIE COLECTATE DE LA PERSOANA VIZATĂ

ÎN CAZUL ÎN CARE PERSOANA VIZATĂ NU ESTE ÎN MĂSURĂ SĂ FURNIZEZE DATELE ȘI ACESTE DATE SUNT NECESARE ÎN SCOPUL PRELUCRĂRII, ACESTEA POT FI COLECTATE DIN ALTE SURSE, DAR CU RESPECTAREA TUTUROR PRINCIPIILOR DE PROTECȚIE A DATELOR

Aceasta este o regulă care îmbunătățește managementul relației cu beneficiarul serviciilor de îngrijire medicală, dar reprezintă și o garanție a exactității datelor, reducând riscul apariției unor date inexacte și a erorilor medicale. Principiul este asumat la nivel european prin Recomandarea Comitetului de Miniștri a Consiliului Europei privind prelucrarea datelor de sănătate.

Texte legale aplicabile: RGPD impune respectarea și aplicabilitatea acestui principiu la articolul 5 alin. 1 lit. a) coroborat cu articolul 6 alin. 4, dar acesta este precizat în mod specific și în numeroase secvențe și ipoteze avute în vedere de legislația națională, în special de **Legea 95/2006 privind reforma în domeniul sănătății, republicată.**

- Spre exemplu, potrivit **articolului 346^1 al Legii 95/2006**, Dosarul electronic de sănătate al pacientului se constituie cu ocazia transmiterii primului document medical al acestuia în DES de către medicii care își desfășoară activitatea în unitățile prevăzute la art. 30 alin. (1), *fără consimțământul pacientului*, realizarea și implementarea acestuia fiind de *utilitate publică de interes naţional*.

- Potrivit **articolului 346^2** utilizarea dosarului electronic de sănătate are drept *scop prioritar creşterea calităţii şi eficienţei actului medical* prin accesul imediat la date şi informaţii medicale, precum şi furnizarea de date şi informaţii statistice necesare politicilor de sănătate, cu implicarea pacientului ca factor activ al protejării şi promovării propriei sănătăţi, prin completarea informaţiilor privind antecedentele personalei fiziologice şi patologicei regim de viaţă, precum şi prin consultarea directă a datelor medicale proprii din dosarul său de sănătate.

Exemplu de bună practică

Într-un centru de urgențe medicale, un pacient este adus în stare gravă și nu poate comunica sau furniza informații despre starea sa medicală. În acest caz, medicul de gardă decide să obțină informațiile medicale necesare ale pacientului de la medicul de familie al acestuia, pentru a asigura un tratament adecvat și în conformitate cu principiile de protecție a datelor.

Centrul de urgențe medicale are politici și proceduri clare privind accesarea datelor medicale ale pacienților în astfel de situații și garantează că acestea sunt respectate. De asemenea, centrul păstrează un registru al accesărilor și prelucrărilor efectuate în astfel de cazuri, pentru a putea fi verificate ulterior și a se asigura că datele personale ale pacienților sunt utilizate numai în scopul tratamentului lor medical.

Cazuistică în domeniu

Curtea de Justiție a Uniunii Europene a judecat în cauza F-46/09 (V & EDPS V. EUROPEAN PARLIAMENT) o cerere de anulare a unei decizii a Parlamentului European prin care se retrage o ofertă de angajare din 2008 făcută reclamantului pe motiv că nu este apt să fie angajat.

Serviciul medical al Comisiei stabilise că reclamanta nu era aptă; aceasta a formulat recurs, iar Comisia a confirmat concluzia. Aceasta a depus o plângere în temeiul articolului 90, pe care Comisia a respins-o, apoi o acțiune în justiție împotriva acestei decizii, pe care Tribunalul de Primă Instanță a respins-o.

În 2008, i s-a propus un post de agent contractual la Parlament. Parlamentul a solicitat și a primit o copie a dosarului său medical de la serviciul medical al Comisiei și, ulterior, și-a retras oferta pe motiv că nu era aptă să lucreze în niciuna dintre instituțiile UE. Reclamanta a depus o plângere împotriva acestei decizii, pe care Parlamentul a respins-o. În acțiunea în fața instanței, reclamanta a susținut că dosarul său medical colectat de Comisie ar fi trebuit să fie utilizat numai în ceea ce privește recrutarea sa de către Comisie. În plus, consilierul medical al Parlamentului ar fi trebuit să o examineze doar pe reclamantă și nu să se intereseze de istoricul său medical anterior.

În memoriul AEPD se afirmă că transferul a încălcat Regulamentul 45/2001. În primul rând, datele nu fac parte din dosarul medical al reclamantei în calitate de fost agent temporar și fost agent contractual al Comisiei. Manualul de procedură al serviciului medical al Comisiei nu indică scopurile pentru care datele medicale colectate în cadrul unei proceduri de recrutare sunt păstrate în arhivă pentru mai mult de 6 luni, nici condițiile în care acestea sunt accesibile.

În avizele adresate Parlamentului și Comisiei a recomandat ca, în cazul candidaților considerați inapți pentru angajare, datele medicale colectate în timpul procedurii de recrutare să fie păstrate doar pentru o perioadă limitată, care să corespundă perioadei în care este posibilă contestarea datelor sau a deciziei luate pe baza acestora. În plus, transferul este reglementat de articolul 7, fără a aduce atingere articolelor 4, 5, 6 și 10. Astfel, respectarea articolului 7 nu face ca transferul și utilizarea finală a datelor să fie legale în temeiul regulamentului în ansamblul său.

În temeiul articolului 10 alineatul (1), prelucrarea unor categorii speciale de date este interzisă, iar protecția acestor date are, pentru CEDO, o importanță fundamentală pentru exercitarea dreptului la viață privată, garantat de articolul 8 din Convenție. Reclamanta nu și-a dat consimțământul pentru transfer, în conformitate cu excepția prevăzută la articolul 10 alineatul (2).

În plus, Parlamentul nu a demonstrat că transferul era cu adevărat necesar pentru respectarea statutului, în sensul articolului 10 alineatul (2) litera (b). Ar fi fost posibil să se obțină informațiile într-un mod mai puțin intruziv. Odată primite de către Parlament, datele nu mai erau utilizate în scopul pentru care au fost colectate. Transferul și utilizarea datelor au încălcat articolul 4 alineatul (1) literele (b) și (e).

Pentru a ilustra pe larg diverse situații relevante specifice acestui principiu, vă rugăm să parcurgeți:

- **Orientarea 3.13** privitoare la **utilizarea datelor cu caracter personal în scopuri secundare decât cele în care au fost colectate inițial**
- **Orientarea 3.16** privind **obținerea și gestionarea consimțământului persoanei vizate**

DATELE PRELUCRATE TREBUIE SĂ FIE ADECVATE, RELEVANTE ȘI LIMITATE LA CEEA CE ESTE NECESAR ÎN RAPORT CU SCOPURILE ÎN CARE SUNT PRELUCRATE

ELE TREBUIE SĂ FIE EXACTE ȘI, ÎN CAZUL ÎN CARE ESTE NECESAR, SĂ FIE ACTUALIZATE

Texte legale aplicabile: RGPD impune respectarea și aplicabilitatea acestui principiu la articolul 5 alin. 1 lit. c) și d), dar acesta este precizat în mod specific și în numeroase secvențe și ipoteze avute în vedere de legislația națională, în special de **Legea 95/2006 privind reforma în domeniul sănătății, republicată**.

- **Articolele 280 și 281 ale Legii 95/2006** stabilește printre atribuțiile CNAS actualizarea Registrului unic de evidență a asiguraților, ceea ce dă expresie garantării principiului exactității datelor cuprinse în acest registru. Această atribuție se realizează pe cale ierarhică, pornind de la competențele teritoriale ale caselor de asigurări de a actualiza datele și a le transmite către CNAS.

- Potrivit **articolului 322 al Legii 95/2006** stabilirea calității de asigurat de către CNAS se face pe baza unor date puse la dispoziție de autoritățile publice pe baza unui protocol. Același protocol stabilește și termenele la care datele sunt actualizate în Platforma informatică din asigurările de sănătate. Chiar dacă același articol stabilește că responsabilitatea pentru corectitudinea datelor revine autorităților publice care le transmit, realitatea este că în temeiul articolului 5 alin. 2 din RGPD răspunderea aparține și CNAS sau caselor de asigurări de sănătate.

- O situație asemănătoare este prevăzută de **articolul 414 al Legii 95/2006**, acesta stabilind că printre atribuțiile CMR se numără și aceea de a actualiza permanent Registrul unic al medicilor.

- Totodată, **articolul 512^1** CMR are atribuția actualizării Registrului unic al medicilor stomatologi din România, informațiile cuprinse în acest titlu fiind colectate, verificate, introduse și actualizate de colegiile teritoriale. Faptul că legea stabilește responsabilitatea pentru realizarea acestor operaţiuni privind membrii înscrişi în colegiul teritorial aparține colegiilor teritoriale, din perspectiva responsabilității față de standardul de protecție a datelor încorporat de RGPD, responsabilitatea revine și CMR.

Exemplu de bună practică în actualizarea datelor medicale

O clinică medicală privată implementează un sistem de gestionare electronică a fișelor medicale ale pacienților. Acest sistem include un mecanism automat de revizuire și actualizare a informațiilor medicale ale pacienților. De exemplu, atunci când un pacient își efectuează analizele de sânge în laborator, rezultatele sunt transmise direct în sistemul informatic al clinicii și sunt adăugate automat la fișa medicală electronică a pacientului.

Clinica are politici și proceduri clare pentru personalul medical, care detaliază pașii necesari pentru a actualiza informațiile medicale ale pacienților. Aceste politici includ instrucțiuni cu privire la revizuirea periodică a informațiilor, verificarea acurateței și corectarea oricăror erori. În plus, clinica instruiește în mod regulat personalul medical în ceea ce privește aceste proceduri, pentru a se asigura că datele medicale ale pacienților sunt actualizate și gestionate corespunzător.

Cazuistică în domeniu

Cauza **P.T. împotriva Republicii Moldova** privește încălcarea regulii confidențialității datelor prin prelucrarea lor disproporționată. Acest caz se referea la dezvăluirea statutului HIV pozitiv al solicitantului într-un certificat care îl scutește de serviciul militar. Reclamantul s-a plâns că a fost nevoit să prezinte certificatul atunci când și-a reînnoit actele de identitate în 2011 și în alte situații, cum ar fi atunci când a solicitat un nou loc de muncă. Curtea a considerat că a avut loc o încălcare a articolului 8 (dreptul la respectarea vieții private) din Convenție, constatând că dezvăluirea faptului că este seropozitiv în armata militară a încălcat dreptul la viață privată al reclamantului. Curtea a remarcat în special că guvernul moldovean nu a specificat care "scop legitim" al articolul 8 din Convenție fusese urmărit prin dezvăluirea bolii reclamantului. În plus, nu au explicat de ce a fost necesar să includă informații sensibile despre reclamant într-un certificat care putea fi solicitat într-o varietate de situații în care starea sa medicală nu era aparent relevantă. În cazul reclamantului, Curtea a considerat că o astfel de ingerință gravă în drepturile sale a fost disproporționată.

Pentru a ilustra pe larg diverse situații relevante specifice acestui principiu, vă rugăm să parcurgeți:

- **Orientarea 3.13** privitoare la **utilizarea datelor cu caracter personal în scopuri secundare decât cele în care au fost colectate inițial**
- **Orientarea 3.16** privind **obținerea și gestionarea consimțământului persoanei vizate**

MĂSURILE DE SECURITATE TREBUIE SĂ FIE ADECVATE, LUÂND ÎN CONSIDERARE CELE MAI RECENTE EVOLUȚII TEHNOLOGICE, NATURA SENSIBILĂ A DATELOR REFERITOARE LA SĂNĂTATE ȘI EVALUAREA RISCURILOR POTENȚIALE

ELE TREBUIE SĂ FIE STABILITE PENTRU A PREVENI RISCURI PRECUM ACCESUL ACCIDENTAL SAU NEAUTORIZAT LA DATELE CU CARACTER PERSONAL, DISTRUGEREA, PIERDEREA, UTILIZAREA, INDISPONIBILITATEA, INACCESIBILITATEA, MODIFICAREA SAU DIVULGAREA

Texte legale aplicabile: RGPD impune respectarea și aplicabilitatea acestui principiu la articolul 5 alin. 1 lit. f), dar acesta este precizat în mod specific și în numeroase secvențe și ipoteze avute în vedere de legislația națională, în special de **Legea 95/2006 privind reforma în domeniul sănătății, republicată**.

- **Articolul 30 al Legii 95/2006** referitor la asistența medicală, stabilește în mod specific pentru cabinete medicale ambulatorii ale medicilor de familie şi de alte specialităţi, centrele de diagnostic şi tratament, centrele medicale, centrele de sănătate, laboratoare, precum şi pentru alte unităţi sanitare publice şi private **obligația asigurării condiţiilor de securitate şi confidenţialitate** în procesul de transmitere a datelor medicale care urmează a fi introduse în dosarul electronic de sănătate a pacientului. Potrivit articolului 30^8 această obligație este pe tot parcursul procedurilor de colectare, prelucrare, utilizare şi stocare a datelor personale.

- Potrivit **articolului 346^4 al Legii 95/2006**, sistemul DES poate face obiectul *interoperabilităţii* cu registrele naționale de sănătate, *în condiţiile legii.*

- Potrivit **articolului 346^5 al Legii 95/2006**, în ceea ce privește prelucrarea datelor în sistemul DES, CNAS are obligația de a adopta *măsuri tehnice şi organizatorice adecvate* în vederea asigurării unui nivel corespunzător de securitate şi confidenţialitate a datelor, în acord cu prevederile art. 32 din Regulamentul general privind protecţia datelor.

- Importanța asigurării securității sistemului DES este reflectată prin aceea că, potrivit **articolului 346^6 al Legii 95/2006**, datele, informaţiile şi procedurile operaţionale necesare utilizării şi funcţionării DES se aprobă prin ordin al ministrului sănătăţii şi al preşedintelui CNAS, cu avizul ministerelor şi instituţiilor din sistemul naţional de apărare, ordine publică şi siguranţă naţională, respectiv Ministerul Apărării Naţionale, Ministerul Afacerilor Interne, Ministerul Justiţiei, Serviciul Român de Informaţii, Serviciul de Telecomunicaţii Speciale, Serviciul de Informaţii Externe, Serviciul de Protecţie şi Pază, în conformitate cu prevederile prezentei legi.

- La **articolul 346^7 al Legii 95/2006** sunt detaliate următoarele măsuri de securitate privind accesul pacienților sau al reprezentanților legali ai acestora la datele şi informaţiile din DES: stabilirea unei matrici de securitate şi a parolei de acces; exclusiv prin intermediul cardului naţional de asigurări sociale de sănătate cu codul PIN asociat acestuia şi a parolei de acces; eliberarea matricei de securitate se face, pe baza solicitării pacienților, de către medicii care deţin un certificat calificat eliberat în condiţiile prevăzute de lege; parola de acces este personalizată de fiecare pacient, este strict confidenţială, fiind un element de securitate cunoscut numai de pacient şi se utilizează în cadrul DES atât pentru cardul naţional de asigurări de sănătate, cât şi pentru matricea de securitate.

- Articolul **933 al Legii 95/2006** cuprinde referințe specifice asigurării securității dispozitivelor medicale și prelucării datelor în conformitate cu RGPD. Astfel, acest articol stabilește pentru utilizatorii dispozitivelor medicale următoarele obligații: de a utiliza dispozitivele medicale numai în scopul pentru care au fost realizate; de a se asigura că dispozitivele medicale sunt utilizate numai în perioada de valabilitate a acestora, când este cazul, şi că nu prezintă abateri de la performanţele funcţionale şi de la cerinţele de securitate aplicabile.

Exemplu de bună practică privind măsurile de securitate adecvate pentru protecția datelor medicale:

Un spital implementează un sistem de management electronic al fișelor medicale ale pacienților și pune în aplicare următoarele măsuri de securitate pentru a proteja datele cu caracter personal și pentru a preveni accesul accidental sau neautorizat, distrugerea, pierderea, utilizarea, indisponibilitatea, inaccesibilitatea, modificarea sau divulgarea:

- **Criptare**: Datele medicale ale pacienților sunt criptate în repaus și în tranzit, utilizând tehnologii de criptare moderne și puternice. Acest lucru asigură că informațiile rămân confidențiale și inaccesibile pentru persoanele neautorizate.
- **Controlul accesului**: Spitalul implementează o politică strictă de control al accesului, care prevede autentificarea cu doi factori pentru a accesa fișele medicale ale pacienților. Personalul medical are acces doar la informațiile necesare îndeplinirii responsabilităților lor profesionale și în conformitate cu principiul accesului minim.
- **Audit și monitorizare**: Sistemul de management al fișelor medicale include funcționalități de audit și monitorizare care înregistrează toate accesările și modificările fișelor medicale. Acest lucru permite identificarea rapidă a oricăror incidente de securitate și a oricăror încălcări ale politicilor de protecție a datelor.
- **Copii de rezervă și planuri de recuperare**: Spitalul efectuează copii de rezervă regulate ale datelor medicale ale pacienților și păstrează aceste copii într-o locație sigură și separată. Spitalul are, de asemenea, un plan de recuperare în caz de dezastre care asigură restaurarea rapidă și sigură a datelor în cazul pierderii sau distrugerii acestora.
- **Pregătirea personalului și actualizarea politicilor**: Spitalul asigură instruirea continuă a personalului medical în ceea ce privește politicile și procedurile de protecție a datelor și de securitate informatică. Aceste politici și proceduri sunt revizuite și actualizate periodic pentru a ține pasul cu evoluțiile tehnologice și pentru a aborda riscurile emergente.
- **Evaluarea riscurilor și testarea de penetrare**: Spitalul efectuează evaluări periodice ale riscurilor în ceea ce privește securitatea datelor medicale și utilizează teste de penetrare realizate de terți independenți pentru a identifica și remedia vulnerabilitățile în sistemul său de management al fișelor medicale.

Prin punerea în aplicare a acestor măsuri, spitalul se asigură că datele medicale ale pacienților sunt protejate în mod adecvat, în conformitate cu principiul menționat.

Cazuistică în domeniu

Speța 1: Incidentul Anthem, Statele Unite ale Americii (2015)

În 2015, Anthem Inc., una dintre cele mai mari companii de asigurări de sănătate din Statele Unite, a suferit o breșă masivă de securitate a datelor, rezultând în expunerea datelor personale și medicale ale aproximativ 78,8 milioane de persoane. Informațiile furate au inclus nume, date de naștere, adrese de e-mail, adrese de domiciliu, numere de asigurare socială, precum și detalii de sănătate.

Această breșă de securitate a reprezentat o încălcare a principiului legalității, transparenței și echității în prelucrarea datelor medicale, deoarece Anthem nu a reușit să protejeze în mod corespunzător informațiile personale și medicale ale pacienților săi, punând în pericol dreptul lor la confidențialitate și protecția datelor.

Ca urmare a incidentului, Anthem a fost investigat de autoritățile federale și statale, precum și de Departamentul de Sănătate și Servicii Umane al SUA (HHS). În 2018, Anthem a ajuns la o înțelegere cu HHS, acceptând să plătească o amendă de 16 milioane de dolari și să adopte un program de conformitate corectivă pentru a îmbunătăți securitatea datelor și a preveni astfel de incidente în viitor.

De asemenea, Anthem a ajuns la o înțelegere într-o acțiune colectivă inițiată de persoanele afectate de breșa de securitate, acceptând să plătească 115 milioane de dolari pentru a acoperi costurile legate de monitorizarea creditului și de protecția împotriva furtului de identitate pentru persoanele afectate.

Această speță reprezintă un exemplu concret de jurisprudență în care s-a constatat încălcarea principiului legalității, transparenței și echității și a securității în prelucrarea datelor medicale.

Speța 2: În 2017, în Statele Unite, firma **Medical Informatics Engineering** (MIE) și afiliata sa **NoMoreClipboard** (NMC), au fost implicate într-un caz de încălcare a datelor medicale.

În acest caz, informații personale și de sănătate ale a aproximativ 3,5 milioane de pacienți au fost expuse în urma unui atac cibernetic. Încălcarea a implicat date sensibile, precum nume, adrese, numere de securitate socială și informații medicale.

În urma investigațiilor, s-a constatat că MIE și NMC nu au implementat măsuri de securitate adecvate pentru a proteja datele pacienților și nu au respectat principiile de protecție a datelor personale.

În ianuarie 2019, MIE a acceptat să plătească o amendă de 100.000 de dolari pentru încălcarea legii federale privind protecția datelor medicale (HIPAA). De asemenea, în 2020, companiile au ajuns la un acord într-un proces colectiv și s-au angajat să plătească 900.000 de dolari pentru a încheia litigiile.

Acest caz a devenit un exemplu renumit privind încălcarea principiilor de protecție a datelor medicale și a subliniat importanța aplicării unor măsuri de securitate adecvate pentru a proteja informațiile sensibile ale pacienților.

Pentru a ilustra pe larg diverse situații relevante specifice acestui principiu, vă rugăm să parcurgeți:

- **Orientarea 3.3** privind **regulile de acces la bazele de date electronice**

TREBUIE RESPECTATE DREPTURILE PERSOANEI ALE CĂREI DATE SUNT PRELUCRATE, ÎN SPECIAL DREPTUL DE ACCES LA DATE ȘI DREPTUL LA INFORMARE, RECTIFICARE, OPOZIȚIE ȘI ȘTERGERE

Texte legale aplicabile: RGPD impune respectarea și aplicabilitatea acestui principiu la articolul 5 alin. 1 lit. f), dar acesta este precizat în mod specific și în numeroase secvențe și ipoteze avute în vedere de legislația națională, în special de **Legea 95/2006 privind reforma în domeniul sănătății, republicată**.

- **Articolul 30^9 al Legii 95/2006** stabilește obligația unităților din sistemul de sănătate de a respecta drepturile pacienților, în special dreptul la informare, de a-şi exprima consimţământul în mod liber şi informat, dreptul la confidențialitate, garantarea securității sistemelor.

- În plus, drepturile pacienților sunt reglementate distinct de **Legea drepturilor pacientului nr. 46/2003**, cu modificările şi completările ulterioare.

- În mod detaliat **Legea 95/2006, la articolul 89**, enumeră categoriile de obligaţii care revin personalului şi cabinetelor de medicină de familie, o categorie distinctă fiind aceea a obligaţiilor faţă de pacienţi - prin îndeplinirea prevederilor specifice din actele normative care reglementează obligaţiile de etică şi deontologie profesională, precum şi din legislaţia privind drepturile pacientului, obligaţiile faţă de sistemul asigurărilor sociale de sănătate.

- Potrivit **articolului 146 al Legii 95/2006** în cazul prelevării de organe, ţesuturi sau celule, drepturile pacienților sunt configurate distinct, demonstrarea respectării acestora fiind obligație concretizată prin întocmirea unui formular specific aprobat prin ordin al ministrului sănătăţii.

- În mod distinct, **la articolul 165**, sunt avute în vedere drepturile pacienților în contextul desfăşurării activităţilor de învăţământ medico-farmaceutic, postliceal, universitar şi postuniversitar, precum şi al activităţilor de cercetare ştiinţifică medicală.

- Printre drepturile pe care le au asiguraţii, **articolul 230** enumeră dreptul la confidențialitate privind datele, în special în ceea ce priveşte diagnosticul şi tratamentul; dreptul la informaţie în cazul tratamentelor medicale.
- **Articolul 234** stabilește dreptul fiecărui asigurat de a fi informat cel puţin o dată pe an, prin casele de asigurări, asupra serviciilor de care beneficiază, precum şi asupra drepturilor şi obligaţiilor sale.
- **Articolul 421 al Legii 95/2006** stabilește obligaţiile membrilor CMR, ce decurg din calitatea lor specială de medici, printre care figurează și aceea de a respecta drepturile pacienților.

Exemplu de bună practică în prelucrarea datelor medicale, respectând drepturile persoanei ale cărei date sunt prelucrate:

O policlinică implementează un portal online securizat pentru pacienți, care le permite acestora să își gestioneze propriile date medicale și să își exercite drepturile în conformitate cu principiile protecției datelor. Următoarele **măsuri** sunt luate pentru a asigura **respectarea drepturilor pacienților:**

- **Accesul la date**: Pacienții se pot autentifica în portalul online securizat, utilizând un sistem de autentificare cu doi factori, pentru a accesa și vizualiza propriile lor fișe medicale.
- **Dreptul la informare**: La prima vizită a unui pacient în clinică, acesta primește un document informativ care explică în detaliu modul în care datele sale medicale vor fi prelucrate, scopul prelucrării, drepturile pe care le are și cum să le exercite.
- **Rectificarea datelor**: Pacienții pot solicita rectificarea oricăror date incorecte sau incomplete prin portalul online sau prin contactarea directă a clinicii. Personalul clinic este instruit să se asigure că astfel de solicitări sunt tratate în mod corespunzător și în timp util.
- **Opoziție**: Pacienții au dreptul să se opună prelucrării datelor lor medicale în anumite circumstanțe, cum ar fi atunci când datele sunt utilizate în scopuri de marketing. Policlinica respectă aceste solicitări și își actualizează politica de confidențialitate pentru a reflecta dreptul pacienților de a se opune.
- **Ștergerea datelor**: Pacienții pot solicita ștergerea datelor lor medicale în anumite situații, cum ar fi atunci când nu mai este necesară păstrarea datelor în scopul pentru care au fost colectate. Clinica se asigură că astfel de solicitări sunt tratate în conformitate cu legislația aplicabilă și într-un mod transparent.

Cazuistică în domeniu

Cauza Avilkina și alții împotriva Rusiei

Reclamanții făceau parte dintr-o organizație religioasă, Centrul administrativ al organizației Martorilor lui Iehova din Rusia. Aceștia au reclamat în special dezvăluirea dosarelor lor medicale către organele de urmărire penală din Rusia, în urma refuzului lor de a li se face transfuzii de sânge în timpul internării lor în spitale publice. În legătură cu deschiderea unei anchete privind legalitatea activităților organizației reclamante, autoritățile de urmărire penală au dat instrucțiuni tuturor spitalelor din Sankt Petersburg să raporteze refuzurile de transfuzii de sânge de către Martorii lui Iehova.

De asemenea, Curtea Europeană a Drepturilor Omului a considerat că a existat o încălcare a articolului 8 (dreptul la respectarea vieții private și de familie) din Convenție în ceea ce privește ceilalți doi reclamanți. Aceasta a constatat, în special, că nu a existat o nevoie socială urgentă de dezvăluire de informații medicale confidențiale despre aceștia. În plus, mijloacele utilizate de către procuror în desfășurarea anchetei, care implică divulgarea de informații confidențiale fără niciun avertisment prealabil sau posibilitatea de a obiecta, nu trebuiau să fie atât de opresive pentru reclamanți.

Prin urmare, autoritățile nu au făcut niciun efort pentru a găsi un echilibru echitabil între, pe de o parte, dreptul reclamanților la respectarea vieții lor private și, pe de altă parte, obiectivul procurorului de a proteja sănătatea publică.

Notă! Acest caz evidențiază aspecte practice și etice extrem de importante, deoarece se poate observa că nici măcar atunci când o solicitare de date medicale este efectuată de un magistrat, transmiterea acestora nu trebuie făcută înainte ca deținătorul să evalueze **necesitatea** transmiterii unor asemenea date, **legalitatea** solicitării, **proporționalitatea** cu obiectivul urmărit de acel magistrat. Ca urmare, **orice medic poate dintr-o perspectivă etică și, mai mult decât atât, bazându-se direct pe principiile R.G.P.D., să refuze orice solicitare de date medicale, indiferent de cine este formulată sau că ar exista un temei legal al acelei solicitări, dacă apreciază că nu este îndeplinit unul dintre criteriile** enunțate mai sus.

Cauza Vilnes și Alții împotriva Norvegiei
Aceasta privește unele reclamații ale scafandrilor că sunt handicapați ca urmare a scufundărilor în Marea Nordului realizate pentru companiile petroliere în perioada de pionierat a explorării petrolului (din 1965 până în 1990). Toți reclamanții s-au plâns de faptul că Norvegia nu a luat măsuri adecvate pentru a proteja sănătatea și viața scafandrilor de mare adâncime atunci când lucrau în Marea Nordului și, în ceea ce privește trei dintre reclamanți, în instalațiile de testare. De asemenea, toți aceștia au susținut că statul nu a reușit să le furnizeze informații adecvate cu privire la riscurile pe care le implică atât scufundările la mare adâncime, cât și cele de testare.

Curtea a considerat că a avut loc o încălcare a articolului 8 (dreptul la respectarea vieții private și a dreptului la viață privată) din Convenție, din cauza faptului că *autoritățile norvegiene nu s-au asigurat ca reclamanții să primească informațiile esențiale care să le permită să evalueze riscurile la sănătatea și viața lor* care rezultă din utilizarea tabelelor de decompresie rapidă. Această cauză completează jurisprudența Curții cu privire la accesul la informații în temeiul articolelor 2 și 8 din Convenție, în special în măsura în care stabilește o *obligație pentru autorități* de *a se asigura că angajații primesc informații esențiale care să le permită să evalueze riscurile profesionale pentru sănătatea și securitatea lor.*

Cauza K.H. și Alții împotriva Slovaciei
Curtea europeană a analizat problematica accesului pacienților la datele lor cu caracter medical, colectate și înregistrate de spitalul de tratament. Reclamantele, opt femei de origine romă, nu au mai putut concepe după ce au fost tratate la secțiile de ginecologie din două spitale diferite și au suspectat că aceasta era din cauză că fuseseră sterilizate în timpul șederii lor în acele spitale. Acestea s-au plâns că nu au putut obține fotocopii ale fișelor lor medicale. Curtea europeană a drepturilor omului a considerat că a avut loc o încălcare a articolului 8 (dreptul la viață privată și familială) din Convenție, întrucât reclamanților nu li s-a permis să facă *fotocopii ale fișelor lor medicale*.

Pentru a ilustra pe larg diverse situații relevante specifice acestui principiu, vă rugăm să parcurgeți:

- **Orientarea 3.10** cu privire la **gestionarea cererilor persoanelor vizate cu privire la propriile informații**
- **Orientarea 3.11** cu privire la **gestionarea reclamațiilor angajaților respectiv pacienților**

II. Principiile privind protecția datelor cu caracter personal (enumerate anterior) ar trebui **să fie luate în considerare implicit** (privacy by default) și **încorporate încă de la proiectarea sistemelor informatice** care prelucrează date referitoare la sănătate (privacy by design). Conformitatea cu aceste principii ar trebui să fie revizuită periodic pe tot parcursul ciclului de viață al prelucrării. Operatorul ar trebui să efectueze, înainte de a începe prelucrarea și la intervale regulate, o **evaluare a impactului potențial al prelucrării** preconizate a datelor în ceea ce privește protecția datelor și respectarea drepturilor omului, inclusiv a măsurilor care vizează reducerea riscului.

Exemplu de bună practică privind respectarea principiilor "privacy by default" și "privacy by design":

O companie care dezvoltă software pentru spitale și alte instituții medicale, să numim această companie "MediTech", a creat un sistem de management electronic al fișelor medicale (EMR) care încorporează principiile de protecție a datelor personale încă de la proiectare. Acest sistem include următoarele caracteristici și măsuri de securitate:

- **Criptarea implicită**: Sistemul utilizează criptarea atât pentru datele aflate în repaus, cât și pentru datele în tranzit, asigurând confidențialitatea și integritatea datelor medicale.
- **Controlul accesului**: Accesul la datele medicale este strict limitat la personalul autorizat, în conformitate cu principiul accesului minim. Acest lucru este realizat prin implementarea unui sistem de autentificare cu doi factori și a unei politici de gestionare a permisiunilor bazată pe **roluri**.
- **Protecție încorporată**: Sistemul include măsuri de protecție încorporate, cum ar fi protecția împotriva atacurilor de tip SQL injection și protecția împotriva accesului neautorizat prin intermediul API-urilor.
- **Evaluarea impactului asupra protecției datelor**: MediTech efectuează evaluări regulate ale impactului asupra protecției datelor pentru a identifica riscurile potențiale și pentru a implementa măsuri de reducere a riscului.
- **Revizuirea periodică a conformității**: MediTech revizuiește periodic conformitatea cu principiile privind protecția datelor și efectuează actualizări ale sistemului EMR pentru a se asigura că rămâne în conformitate cu legislația și reglementările aplicabile.
- **Formarea și informarea utilizatorilor**: MediTech oferă instruire și suport pentru personalul medical care utilizează sistemul EMR, subliniind importanța protecției datelor personale și explicând modul în care sistemul asigură respectarea acestor principii.

Prin implementarea acestor măsuri și caracteristici în sistemul său de management electronic al fișelor medicale, MediTech asigură respectarea principiilor "privacy by default" și "privacy by design" și protejează datele medicale ale pacienților în conformitate cu legislația și reglementările privind protecția datelor.

Cazuistică în domeniu

Cazul Municipiul Bergen, Norvegia (2019)

La 19 martie, Autoritatea norvegiană pentru protecția datelor a aplicat o amendă administrativă de 1,6 milioane de coroane norvegiene, echivalentul a 170.000 de euro, municipalității din Bergen.

Incidentul se referă la fișierele informatice din sistemul informatic al municipalității, care conțineau datele personale a peste 35 000 de elevi și angajați ai școlilor primare ale municipalității. Din cauza unor măsuri de securitate insuficiente, aceste fișiere erau neprotejate și accesibile în mod deschis oricărui utilizator al sistemului, indiferent de tipul de autorizație. Acest lucru a permis utilizatorilor neautorizați să acceseze diversele sisteme informatice și datele personale ale școlii. Faptul că majoritatea persoanelor afectate erau copii și că municipalitatea a fost avertizată de mai multe ori (atât de către autoritate, cât și de către un denunțător intern) au fost considerate factori agravanți. Municipalitatea nu a făcut apel la decizie.

Autoritatea de supraveghere a datelor a constatat că municipiul Bergen nu a respectat principiile "privacy by design" și "privacy by default", întrucât nu a implementat măsuri tehnice și organizatorice adecvate pentru a proteja datele personale ale utilizatorilor. Concret, municipiul nu a asigurat restricționarea accesului la informațiile respective numai pentru personalul autorizat și nu a implementat mecanisme adecvate de autentificare și autorizare în sistemul său.

Acest caz demonstrează importanța implementării corespunzătoare a principiilor "privacy by design" și "privacy by default" în sistemul de prelucrare a datelor și consecințele nerespectării acestor principii în conformitate cu GDPR.

Cazul Haga District Court, Olanda (2019)

Autoritatea olandeză pentru protecția datelor ("AP") a anunțat, la 16 iulie 2019, că a impus o amendă de 460 000 EUR societății Stichting HagaZiekenhuis pentru încălcări ale securității în temeiul articolului 32 din Regulamentul general privind protecția datelor [Regulamentul (UE) 2016/679] ("GDPR").

În special, AP a evidențiat faptul că spitalul nu a pus în aplicare măsuri de securitate internă adecvate pentru a proteja dosarele pacienților, lucru care a fost dezvăluit după ce personalul medical a accesat fără motiv dosarele unui cunoscut cetățean olandez, ceea ce a dus la o anchetă.

În plus, AP a remarcat că, în cazul în care spitalul nu își îmbunătățește măsurile de securitate până la 2 octombrie 2019, va fi, de asemenea, supus unei sancțiuni de 100 000 euro la fiecare două săptămâni, cu un maxim de 300 000 euro. AP a subliniat că spitalul nu a reușit să implementeze controale cu privire la cine are posibilitatea de a accesa dosarele pacienților și să pună în aplicare un sistem care să necesite cel puțin autentificarea cu doi factori.

Deși acest caz nu se referă în mod specific la principiile "privacy by design" și "privacy by default", el subliniază importanța securității datelor în sectorul medical și consecințele nerespectării GDPR în acest context.

III. Operatorii de date și persoanele împuternicite care acționează sub responsabilitatea acestora ar trebui să ia toate măsurile adecvate pentru a-și îndeplini obligațiile în ceea ce privește protecția datelor și ar trebui să fie în măsură **să demonstreze** în special pentru autoritatea de supraveghere competentă că prelucrarea este în **conformitate** cu aceste obligații.

Exemplu de bună practică privind respectarea obligațiilor de protecție a datelor de către un spital:

Spitalul "XYZ" a implementat un program cuprinzător de conformitate cu protecția datelor pentru a se asigura că prelucrarea datelor personale, inclusiv a datelor medicale sensibile, este în conformitate cu legislația aplicabilă și cu GDPR. Acest program include următoarele componente:

- **Desemnarea unui responsabil cu protecția datelor (DPO)**: Spitalul a numit un DPO care supraveghează toate activitățile legate de protecția datelor și asigură conformitatea cu GDPR.
- **Politici și proceduri interne**: Spitalul a elaborat politici și proceduri clare și detaliate privind prelucrarea datelor personale, care sunt puse la dispoziția tuturor angajaților și colaboratorilor.
- **Formare și conștientizare**: Spitalul oferă instruire periodică angajaților și colaboratorilor cu privire la protecția datelor și responsabilitățile lor în cadrul programului de conformitate.
- **Controlul accesului și securitatea datelor**: Spitalul a implementat măsuri tehnice și organizatorice adecvate pentru a proteja datele personale, cum ar fi controlul accesului bazat pe roluri, criptarea datelor și monitorizarea activității în sistemele informatice.
- **Evaluarea impactului asupra protecției datelor (DPIA)**: Spitalul efectuează evaluări ale impactului asupra protecției datelor pentru orice prelucrare de date care prezintă un risc înalt pentru drepturile și libertățile persoanelor fizice.
- **Înregistrarea activităților de prelucrare**: Spitalul menține un registru al activităților de prelucrare a datelor, care include detalii despre scopul, natura și categoriile de date personale prelucrate.
- **Notificarea încălcărilor de securitate**: Spitalul a stabilit proceduri pentru notificarea promptă a încălcărilor de securitate către autoritatea de supraveghere competentă și persoanele vizate, conform cerințelor GDPR.

- **Monitorizarea și revizuirea periodică**: Spitalul efectuează revizuiri și audituri periodice ale programului său de conformitate cu protecția datelor pentru a identifica și aborda eventualele deficiențe și a se asigura că rămâne în conformitate cu legislația și reglementările aplicabile.

Prin implementarea acestui program cuprinzător de conformitate cu protecția datelor, spitalul "XYZ" își îndeplinește obligațiile în ceea ce privește protecția datelor și poate demonstra autorității de supraveghere competente că prelucrarea datelor personale este în conformitate cu aceste obligații.

Pentru a ilustra pe larg diverse situații relevante specifice acestui principiu, vă rugăm să parcurgeți:

- **Orientarea 3.12** privind **modalitatea de răspuns în caz de încălcare a securității și confidențialității datelor pacientului sau a altei persoane vizate**

IV. Operatorii de date și persoanele împuternicite de către aceștia care nu sunt profesioniști din domeniul sănătății ar trebui să prelucreze datele referitoare la sănătate **numai în conformitate cu normele de confidențialitate și măsurile de securitate** care asigură un nivel de protecție **echivalent celui impus profesioniștilor din domeniul sănătății.**

Exemplu de bună practică privind respectarea normelor de confidențialitate și măsurile de securitate de către spitale pentru operatorii de date și persoanele împuternicite care nu sunt profesioniști din domeniul sănătății:

Spitalul "ABC" lucrează cu o companie externă de facturare și procesare a plăților, care are acces la anumite date referitoare la sănătate ale pacienților în scopul facturării serviciilor medicale. Pentru a asigura respectarea normelor de confidențialitate și a măsurilor de securitate, spitalul "ABC" și compania de facturare au implementat următoarele măsuri:

- **Acord de confidențialitate**: Spitalul "ABC" și compania de facturare au încheiat un acord de confidențialitate care prevede obligațiile părților în ceea ce privește protecția datelor referitoare la sănătate și responsabilitățile legate de păstrarea confidențialității acestor date.
- **Controlul accesului**: Compania de facturare are acces limitat la datele referitoare la sănătatea pacienților și poate prelucra aceste date numai în scopurile prealabile stabilite, cum ar fi facturarea și procesarea plăților. Accesul la date este restricționat în funcție de rolurile angajaților și necesitățile legitime de a accesa aceste informații.
- **Formare și conștientizare**: Spitalul "ABC" și compania de facturare oferă instruire periodică angajaților care lucrează cu date referitoare la sănătate în ceea ce privește normele de confidențialitate, măsurile de securitate și responsabilitățile lor în cadrul GDPR și a legislației naționale privind protecția datelor.
- **Măsuri tehnice și organizatorice de securitate**: Compania de facturare implementează măsuri de securitate adecvate pentru a proteja datele referitoare la sănătate, cum ar fi criptarea datelor în tranzit și la repaus, monitorizarea activității în sistemele informatice și protejarea fizică a serverelor și echipamentelor.
- **Audituri și revizuiri periodice**: Spitalul "ABC" efectuează audituri și revizuiri periodice ale măsurilor de confidențialitate și securitate implementate de compania de facturare pentru a se asigura că acestea respectă normele și măsurile de protecție adecvate.

Cazuistică în domeniu

Autoritatea Națională de Supraveghere din România a finalizat în luna februarie a anului curent (2023) o investigație la operatorul Tehnoplus Industry SRL în cadrul căreia a constatat încălcarea prevederilor art. 5 alin. (1) lit. a), c), e) și alin. (2), precum și ale art. 6 din Regulamentul General privind Protecția Datelor (RGPD) și a sancționată cu o amendă de aproximativ 5000 EURO.

Investigația s-a desfășurat ca urmare a unei plângeri prin care se reclama faptul că operatorul a prelucrat datele cu caracter personal ale petentului prin intermediul sistemului GPS instalat pe mașina sa de serviciu, fără să fi fost informat cu privire la monitorizarea autovehiculului, scopul și temeiul legal al acestei prelucrări și durata de stocare a datelor astfel colectate.

De asemenea, petentul a mai reclamat faptul că informațiile extrase din sistemul GPS au fost utilizate de operator în alt scop decât acela de a monitoriza mașina de serviciu atribuită acestuia.

În cadrul investigației efectuate s-a constatat faptul că Tehnoplus Industry SRL a prelucrat în mod excesiv (în afara orelor de serviciu) datele de localizare aferente petentului, angajat al operatorului, prin sistemul de monitorizare GPS instalat pe mașina acestuia de serviciu, fără să fi demonstrat că anterior a epuizat alte metode mai puțin intruzive pentru atingerea scopului prelucrării și fără a face dovada informării complete a petentului în legătură cu prelucrarea datelor prin intermediul sistemului GPS, încălcând astfel prevederile art. 5 alin. (1) lit. a), c) și (2) și art. 6 din RGPD.

Totodată, s-a constatat că operatorul a stocat datele din sistemul mai sus menționat, după expirarea duratei de stocare, fără să prezinte dovezi din care să rezulte că depășirea termenului de 30 de zile prevăzut de art. 5 din Legea nr. 190/2018 se bazează pe motive justificate, încălcând astfel dispozițiile art. 5 alin. (1) lit. e) și (2) din RGPD.

De asemenea, s-a constatat că operatorul a utilizat datele petentului din sistemul GPS în alt scop decât cel pentru care le colectase inițial.

În același timp, în temeiul art. 58 alin. (2) lit. d) din RGPD, s-au dispus față de societatea Tehnoplus Industry SRL:

- măsura corectivă de a asigura conformitatea cu RGPD a operațiunilor de colectare și prelucrare ulterioară a datelor personale, prin reevaluarea necesității atingerii scopurilor propuse prin folosirea datelor de localizare provenite din sistemul de monitorizare prin GPS instalate pe mașinile de serviciu ale angajaților operatorului și evitarea colectării excesive a datelor, prin raportare la obligațiile prevăzute de RGPD și de Legea nr. 190/2018;

- măsura corectivă de a asigura conformitatea cu RGPD a operațiunilor de colectare și prelucrare ulterioară a datelor personale, prin limitarea perioadei de stocare a datelor prin raportare la scopurile prelucrării datelor, conform obligațiilor prevăzute de RGPD și de Legea nr. 190/2018.

Pentru a ilustra pe larg diverse situații relevante specifice acestui principiu, vă rugăm să parcurgeți:

- **Orientarea 3.14 privind distrugerea în siguranță a datelor cu caracter personal**

4.4 TEMEIURILE LEGITIME ȘI SITUAȚII SPECIALE ALE PRELUCRĂRILOR DE DATE

TEMEIURILE LEGITIME ALE PRELUCRĂRII DATELOR PRIVIND SĂNĂTATEA

Prelucrarea este legală numai dacă și în măsura în care operatorul se poate baza **pe cel puțin unul dintre temeiurile legitime descrise la punctele A, B, C și D**. În același timp, în toate cazurile, ar trebui să se stabilească garanții adecvate pentru securitatea datelor și respectarea drepturilor persoanelor fizice. Orice alte garanții pot fi prevăzute de lege în vederea salvgardării respectării drepturilor și libertăților fundamentale.

Gruparea situațiilor legitime de prelucrare s-a realizat în funcție de sursa care a generat prelucrarea. Astfel, **primele trei categorii au în centrul lor o manifestare inițială a voinței** persoanei vizate / pacientului în ceea ce privește prelucrarea datelor sale sau cel puțin voința acestuia s-a aflat în parte la originea prelucrării datelor sale; **ultima categorie este aceea care grupează toate situațiile** în care prelucrarea datelor personale, în special a celor de sănătate, se realizează ca o consecință directă sau indirectă fie a legii, fie a unor evenimente sau interese de o importanță sau intensitate mai ridicate.

A. Datele referitoare la sănătate pot fi prelucrate dacă **persoana vizată și-a dat consimțământul**, cu excepția cazurilor în care legea prevede că o interdicție privind prelucrarea datelor referitoare la sănătate nu poate fi ridicată doar prin consimțământul persoanei vizate. În cazul în care este necesar consimțământul persoanei vizate pentru prelucrarea datelor referitoare la sănătate, în conformitate cu legea, acesta trebuie să fie liber, specific, informat și explicit. Persoana vizată este informată cu privire la dreptul său de a-și retrage consimțământul în orice moment și este informată că o astfel de retragere nu va afecta legalitatea prelucrării efectuate pe baza consimțământului său înainte de retragere. Retragerea consimțământului trebuie să fie la fel de ușoară ca și acordarea acestuia.

B. Datele referitoare la sănătate pot fi prelucrate în cazul în care **prelucrarea este necesară pentru executarea unui contract** încheiat de persoana vizată sau în numele acesteia cu un profesionist din domeniul sănătății, sub rezerva condițiilor definite de lege, inclusiv a obligației de păstrare a secretului.

C. Datele referitoare la sănătate făcute publice în mod evident de către persoana vizată pot fi prelucrate.

D. Prelucrarea este necesară pentru:

- scopuri de medicină preventivă și în scopuri de diagnosticare medicală, de administrare a îngrijirii sau a tratamentului sau de gestionare a serviciilor de sănătate de către profesioniștii din domeniul sănătății și cei din sectoarele de asistență medicală și socială, în condițiile prevăzute de lege
- din **motive de sănătate publică**, cum ar fi protecția împotriva pericolelor pentru sănătate, acțiuni umanitare sau pentru a asigura un standard ridicat de calitate și siguranță a tratamentelor medicale, a produselor medicale și a dispozitivelor medicale, în condițiile prevăzute de lege
- în scopul **protejării intereselor vitale ale persoanei vizate sau ale unei alte persoane**, în cazul în care consimțământul nu poate fi obținut
- motive legate de **obligațiile operatorilor și de exercitarea drepturilor acestora sau ale persoanei vizate în materie de ocupare a forței de muncă și de protecție socială**, în conformitate cu legea sau cu orice contract colectiv de muncă care o respectă
- motive de **interes public în domeniul gestionării cererilor de prestații și servicii de asigurări sociale și de sănătate**, în condițiile prevăzute de lege

- prelucrarea în scopuri de **arhivare în interes public** sau în scopuri de **cercetare științifică sau istorică sau de statistică**, în condițiile definite de lege pentru a garanta protecția drepturilor fundamentale și a intereselor legitime ale persoanei vizate
- motive esențiale pentru recunoașterea, exercitarea sau **apărarea unui drept legal**
- din motive de **interes public substanțial**, în temeiul legii, care trebuie să fie proporționale cu scopul urmărit, să respecte esența dreptului la protecția datelor și să prevadă măsuri adecvate și specifice de protecție a drepturilor fundamentale și a intereselor persoanei vizate

SITUAȚII ȘI CATEGORII SPECIALE DE DATE DIN DOMENIUL SĂNĂTĂȚII

A. Datele privind copiii nenăscuți

Datele referitoare la sănătate privind copiii nenăscuți, cum ar fi datele care rezultă dintr-un diagnostic prenatal sau din identificarea caracteristicilor genetice ale unor astfel de copii, ar trebui să beneficieze de o protecție adecvată.

B. Datele genetice legate de sănătate

Datele referitoare la sănătate privind copiii nenăscuți, cum ar fi datele care rezultă dintr-un diagnostic prenatal sau din identificarea caracteristicilor genetice ale unor astfel de copii, ar trebui să beneficieze de o protecție adecvată.

- Datele genetice trebuie să fie colectate **numai sub rezerva unor garanții adecvate** și în cazul în care acestea sunt **prevăzute de lege sau pe baza consimțământului** exprimat de persoana vizată, cu excepția cazului în care consimțământul este exclus prin lege ca temei juridic pentru prelucrarea datelor genetice.
- Datele genetice prelucrate în scop preventiv, pentru diagnosticarea sau pentru tratamentul persoanei vizate sau al unui membru al familiei biologice al acesteia sau pentru cercetare științifică trebuie să fie utilizate numai în aceste scopuri sau pentru a permite persoanelor vizate de rezultatele acestor teste să ia o decizie în cunoștință de cauză cu privire la aceste aspecte.

- Prelucrarea datelor genetice în scopul unei proceduri sau al unei anchete judiciare trebuie să fie utilizată numai atunci **când nu există mijloace alternative sau mai puțin intruzive** pentru a stabili dacă există o legătură genetică în contextul producerii de probe, pentru a preveni un pericol real și imediat sau pentru urmărirea penală a unei infracțiuni specifice, sub rezerva unor garanții procedurale adecvate. Astfel de date nu trebuie să fie utilizate pentru a determina alte caracteristici care pot avea o legătură genetică, cu excepția cazului în care sunt prevăzute prin lege garanții adecvate.

- Prelucrarea datelor genetice poate fi utilizată în scopul identificării persoanelor în cadrul unei **crize sau al unei acțiuni umanitare**, în cazul în care sunt prevăzute de lege garanții adecvate.

- Datele predictive existente rezultate din testele genetice nu trebuie să fie prelucrate în scopuri de asigurare, cu excepția cazului în care acest lucru este prevăzut în mod specific de lege. În acest caz, prelucrarea acestora ar trebui să fie **autorizată numai cu respectarea deplină a criteriilor aplicabile definite de lege**, în funcție de tipul de test utilizat și de riscul specific în cauză.

- Persoana vizată are dreptul de a cunoaște orice informație referitoare la datele sale genetice, sub rezerva situațiilor când legea stabilește explicit că această obligație nu există în sarcina operatorului, iar măsura este necesară într-o societate democratică și este proporțională cu obiectivul urmărit. Cu toate acestea, persoana vizată poate avea propriile motive pentru a **nu dori să cunoască** anumite aspecte legate de sănătate și toată lumea ar trebui să fie conștientă, înainte de orice analiză, de posibilitatea de a nu fi informată cu privire la rezultate, inclusiv în cazul unor rezultate neașteptate. În circumstanțe excepționale, dorința acestora de a nu ști ar putea fi limitată, așa cum prevede legea, în special în interesul propriu al persoanei vizate sau în lumina obligației medicilor de a acorda îngrijire.

C. Schimbul de date referitoare la sănătate în scopul furnizării și administrării asistenței medicale

- În cazul în care datele referitoare la sănătate sunt partajate de diferiți profesioniști în scopul furnizării și administrării de asistență medicală unei persoane, persoana vizată este **informată în prealabil**, cu excepția cazului în care acest lucru se dovedește imposibil din cauza unei urgențe sau când persoana vizată dispune deja de informațiile necesare. În plus, în cazul în care datele cu caracter personal nu sunt colectate direct de la persoana vizată,

operatorul nu este obligat să o informeze în cazul în care prelucrarea este prevăzută în mod expres de lege sau dacă acest lucru se dovedește a fi imposibil, de exemplu atunci când datele de contact ale persoanei fizice s-au schimbat, iar persoana fizică nu poate fi găsită sau nu poate fi contactată, sau implică eforturi disproporționate din partea operatorului, în special pentru prelucrarea în scopuri de arhivare în interes public și pentru scopuri de cercetare științifică sau istorică sau în scopuri statistice. În cazul în care schimbul de date se bazează pe consimțământul persoanei vizate, acesta poate fi retras în orice moment. În cazul în care schimbul de date este autorizat prin lege, persoana vizată se poate opune schimbului de date privind sănătatea sa.

- Profesioniștii care lucrează la un anumit caz individual în sectorul asistenței medicale și al asistenței sociale și care fac schimb de date în interesul unei mai bune coordonări pentru a asigura calitatea asistenței medicale ar trebui să facă obiectul **confidențialității profesionale care îi revine unui profesionist** din domeniul asistenței medicale sau al unor norme de confidențialitate de același nivel.

- Schimbul și partajarea de date între profesioniștii din domeniul sănătății ar trebui **să se limiteze la informațiile strict necesare** pentru coordonarea sau continuitatea îngrijirii, prevenirea sau monitorizarea medico-socială și socială a individului. Profesioniștii din domeniul sănătății respectivi pot, în acest caz, să facă schimb de date sau să primească date numai în cadrul sarcinilor lor și în funcție de autorizațiile lor. Trebuie să se ia măsuri adecvate pentru a se asigura securitatea datelor.

- Utilizarea unui dosar medical electronic și a unei căsuțe poștale electronice care să permită partajarea și schimbul de date referitoare la sănătate trebui **să respecte toate principiile** și regulile de protecție a datelor, deja menționate.

- În cadrul schimbului și al partajării datelor referitoare la sănătate, trebuie adoptate **măsuri de securitate fizică, tehnică și administrativă**, precum și cele necesare pentru a garanta confidențialitatea, integritatea și disponibilitatea datelor referitoare la sănătate.

D. Comunicarea de date referitoare la sănătate în alte scopuri decât furnizarea și administrarea de asistență medicală

- Datele referitoare la sănătate pot fi **comunicate destinatarilor** care sunt autorizați prin lege să aibă acces la aceste date.

- **Companiile** de asigurări **nu pot fi considerate drept destinatari autorizați** să aibă acces la datele referitoare la sănătate ale persoanelor fizice, cu excepția cazului în care legea prevede acest lucru cu garanții adecvate și în conformitate cu principiile de protecție a datelor.

- **Angajatorii nu pot fi considerați drept destinatari autorizați** să aibă acces la datele privind sănătatea persoanelor fizice, cu excepția situațiilor strict reglementate de lege, necesare pentru prelucrarea datelor cu caracter personal în contextul relațiilor de muncă.

- **Datele referitoare la sănătate pot fi comunicate numai unui destinatar autorizat** care este supus normelor de confidențialitate care revin unui profesionist din domeniul sănătății sau unor norme de confidențialitate echivalente, cu excepția cazului în care legea prevede alte garanții adecvate.

E. Stocarea datelor referitoare la sănătate

Datele referitoare la sănătate **nu ar trebui să fie stocate într-o formă care să permită identificarea persoanelor vizate** pentru o perioadă mai lungă decât cea necesară pentru scopurile în care sunt prelucrate, cu excepția cazului în care sunt utilizate în scopuri de arhivare în interes public sau în scopuri de cercetare științifică sau istorică sau în scopuri statistice și în cazul în care există măsuri adecvate pentru a proteja drepturile și libertățile fundamentale ale persoanei vizate. În acest caz, datele ar trebui, în principiu, să fie **anonimizate** de îndată ce cercetarea, activitatea de arhivare sau studiul statistic permite acest lucru.

F. Securitatea și interoperabilitatea

- **Securitatea**
    - Prelucrarea datelor referitoare la sănătate trebuie să fie **securizată**. În acest sens, trebuie definite și puse în aplicare măsuri de securitate adaptate la riscurile pentru drepturile omului și libertățile fundamentale, pentru a se asigura că toate părțile interesate respectă standarde ridicate care să garanteze legalitatea prelucrării, precum și securitatea și confidențialitatea acestor date.

- Dispozițiile privind securitatea datelor, prevăzute de lege sau de alte reglementări și cuprinse în cadrele de referință, după caz, trebuie să aibă ca rezultat **măsuri tehnice și organizatorice de ultimă generație**, revizuite periodic, astfel încât să protejeze datele cu caracter personal referitoare la sănătate de orice distrugere ilegală sau accidentală, de orice pierdere sau de orice alterare și să se protejeze împotriva oricărui acces neautorizat, a indisponibilității sau a inaccesibilității. În special, legea ar trebui să prevadă dispoziții pentru organizarea și reglementarea procedurilor privind colectarea, stocarea și restituirea datelor referitoare la sănătate.

- **Disponibilitatea** sistemului, ceea ce înseamnă o bună funcționare a sistemului, trebuie să fie asigurată prin măsuri care să permită accesul la date într-un mod sigur și ținând seama în mod corespunzător de nivelul de permisiune al persoanelor autorizate.

- **Garantarea integrității** presupune verificarea acțiunilor efectuate asupra datelor, a oricăror modificări aduse datelor sau a ștergerii acestora, inclusiv a comunicării datelor. Aceasta presupune, de asemenea, instituirea de măsuri de monitorizare a accesului la baza de date și la datele în sine, asigurându-se că numai persoanele autorizate pot avea acces la date.

- **„Auditabilitatea”** ar trebui să conducă la un sistem în care să fie posibilă urmărirea oricărui acces la sistemul de informații, a modificărilor efectuate și a oricărei acțiuni desfășurate, în vederea identificării autorului acesteia.

- Activitatea care implică găzduirea în exterior a datelor referitoare la sănătate și punerea lor la dispoziția utilizatorilor ar trebui să respecte **cadrul de referință în materie** de securitate și principiile de protecție a datelor cu caracter personal.

- Profesioniștii care nu sunt direct implicați în îngrijirea sănătății persoanei, dar care, în virtutea sarcinilor care le sunt atribuite, asigură buna funcționare a sistemelor informatice, pot avea acces, **în măsura în care este necesar** pentru îndeplinirea sarcinilor lor și în mod ad-hoc, la datele cu caracter personal referitoare la sănătate. Aceștia trebuie să respecte pe deplin secretul profesional și să se conformeze măsurilor adecvate prevăzute de lege pentru a garanta confidențialitatea și securitatea datelor.

- **Interoperabilitatea**
  - Interoperabilitatea poate contribui la satisfacerea unor nevoi importante în sectorul sănătății și poate oferi mijloace tehnice pentru a facilita actualizarea informațiilor sau pentru a evita stocarea de date identice în mai multe baze de date, precum și pentru a contribui la portabilitatea datelor.

  - Cu toate acestea, este necesar ca interoperabilitatea să fie pusă în aplicare cu respectarea deplină a principiilor de protecție a datelor, în special a principiilor legalității, necesității și proporționalității, și ca, atunci când se utilizează sisteme interoperabile, să se instituie garanții de protecție a datelor.

  - Cadrele de referință bazate pe norme internaționale care oferă o structură tehnică ce facilitează interoperabilitatea ar trebui să garanteze un nivel ridicat de securitate, asigurând în același timp o astfel de interoperabilitate. Monitorizarea punerii în aplicare a unor astfel de cadre de referință poate fi realizată prin intermediul unor sisteme de certificare.

- **Cercetarea științifică**
  - Prelucrarea datelor referitoare la sănătate în scopul cercetării științifice ar trebui să facă obiectul unor garanții adecvate prevăzute de lege, să fie efectuată cu un scop legitim și să fie în conformitate cu drepturile și libertățile fundamentale ale persoanei vizate.

  - Necesitatea prelucrării datelor privind sănătatea în scopul cercetării științifice ar trebui să fie evaluată în funcție de scopurile proiectului de cercetare, de riscurile pentru persoana vizată și, în ceea ce privește prelucrarea datelor genetice, în funcție de riscul pentru familia biologică.

  - În principiu, datele referitoare la sănătate ar trebui să fie prelucrate în cadrul unui proiect de cercetare științifică numai dacă persoana vizată și-a dat consimțământul liber, explicit, specific și informat. Cu toate acestea, legea poate prevedea prelucrarea datelor referitoare la sănătate pentru cercetare științifică fără consimțământul persoanei vizate.

- Condițiile în care datele referitoare la sănătate sunt prelucrate pentru cercetare științifică trebuie să fie evaluate, dacă este necesar, de către un organism independent cu atribuții în acest sens, cum ar fi, spre exemplu, un comitet de etică alcătuit din experți independenți.

- Profesioniștii din domeniul sănătății care au dreptul de a efectua propriile cercetări medicale și oamenii de știință din alte discipline ar trebui să poată utiliza datele referitoare la sănătate pe care le dețin, atât timp cât persoana vizată a fost informată în prealabil cu privire la această posibilitate și sub rezerva unor garanții complementare stabilite prin lege, cum ar fi solicitarea consimțământului explicit sau evaluarea organismului competent desemnat prin lege.

- În cazul în care scopurile de cercetare științifică permit acest lucru, datele ar trebui să fie anonimizate; în cazul în care scopurile de cercetare nu permit acest lucru, pseudonimizarea datelor - cu intervenția unei terțe părți de încredere în etapa de separare a identificării - se numără printre măsurile care ar trebui puse în aplicare pentru a proteja drepturile și libertățile fundamentale ale persoanei vizate. Aceste măsuri trebuie să fie aplicate în cazul în care scopurile cercetării științifice pot fi îndeplinite prin prelucrarea ulterioară care nu permite sau nu mai permite identificarea persoanelor vizate.

- În cazul în care o persoană vizată se retrage dintr-un proiect de cercetare științifică, datele sale privind sănătatea prelucrate în contextul cercetării respective ar trebui să fie distruse sau anonimizate într-un mod care să nu compromită validitatea științifică a cercetării, iar persoana vizată ar trebui să fie informată în consecință.

- Datele cu caracter personal utilizate pentru cercetarea științifică nu ar trebui să fie publicate într-o formă care să permită identificarea persoanei vizate, cu excepția următoarelor situații:
    - în cazul în care persoana vizată și-a dat consimțământul pentru aceasta; sau
    - în cazul în care legea permite o astfel de publicare cu condiția ca aceasta să fie indispensabilă pentru prezentarea rezultatelor cercetării privind evenimente contemporane și numai în măsura în care interesul publicării datelor prevalează asupra intereselor și drepturilor și libertăților fundamentale ale persoanei vizate.

- **Dispozitive mobile**
    - În cazul în care datele colectate de dispozitivele mobile, implantate sau nu în persoana fizică, pot dezvălui informații privind starea fizică sau psihică a unei persoane în legătură cu sănătatea și bunăstarea acesteia sau se referă la orice informații privind furnizarea de asistență medicală și socială, acestea constituie date referitoare la sănătate. În acest sens, acestea ar trebui să se bucure de aceeași protecție juridică și de aceeași confidențialitate aplicabile altor prelucrări de date privind sănătatea.

    - Persoanele care utilizează astfel de dispozitive mobile care implică prelucrarea datelor lor cu caracter personal ar trebui să beneficieze de aceleași drepturi ca cele prevăzute pentru pacienți și reglementate de legea privind drepturile pacientului și în legea prin reforma în domeniul sănătății. Acestora trebuie, în special, să li se fi furnizat în prealabil toate informațiile necesare privind natura și funcționarea sistemului pentru a putea controla utilizarea acestuia. În acest scop, informații clare și transparente privind prelucrarea preconizată trebuie să fie redactate de către operator cu participarea proiectantului de software și a distribuitorului de software, ale căror roluri respective trebuie să fie stabilite în prealabil.

    - Orice utilizare a dispozitivelor mobile trebuie să fie însoțită de măsuri de securitate specifice, personalizate și de ultimă generație, care să prevadă în special autentificarea persoanei în cauză și criptarea transmiterii de date.

    - Găzduirea externă a datelor referitoare la sănătate produse de dispozitivele mobile trebuie să se supună unor norme de securitate care să prevadă confidențialitatea, integritatea și restituirea datelor la cererea persoanei vizate.

Protecția fluxurilor transfrontaliere de date referitoare la sănătate

Fluxurile transfrontaliere de date pot avea loc numai în cazul în care se asigură un nivel adecvat de protecție a datelor în conformitate cu garanțiile prevăzute în Regulamentul General privind Protecția Datelor și în Convenția 108+ sau pe baza următorului regim de derogări care vizează să permită un transfer către un destinatar care nu asigură un nivel adecvat de protecție:

- persoana vizată și-a dat consimțământul explicit, specific și liber pentru transfer, după ce a fost informată cu privire la riscurile care apar în absența unor garanții adecvate
- interesele specifice ale persoanei vizate impun acest lucru în cazul respectiv
- interesele legitime predominante, în special interesele publice importante, sunt prevăzute de lege și un astfel de transfer constituie o măsură necesară și proporțională într-o societate democratică
- transferul constituie o măsură necesară și proporțională pentru libertatea de exprimare într-o societate democratică

4.5 DREPTURILE PERSOANEI VIZATE

Drepturile persoanei vizate, aceasta fiind de regulă pacientul, sunt complet **legate de principiile de prelucrare a datelor cu caracter personal**, deoarece dacă ar fi să facem o comparație de stil, conceptul de „drepturi ale persoanei vizate” se vede în oglindă drept conceptul de „principii de prelucrare a datelor cu caracter personal”.

A. Drepturi asigurate de principiul transparenței prelucrării datelor personale

- Operatorul trebuie **să informeze** persoana vizată cu privire la prelucrarea datelor sale referitoare la sănătate
- Informațiile trebuie **să includă cel puțin**:
    - identitatea și datele de contact ale operatorului (ex. cabinet) și ale persoanelor împuternicite de operator[1] [2] (ex. furnizorul unei aplicații informatice), dacă este cazul
    - scopul în care sunt prelucrate datele și, dacă este cazul, temeiul juridic relevant pentru acesta
    - durata de păstrare a datelor
    - destinatarii sau categoriile de destinatari ai datelor, precum și transferurile de date planificate către o țară terță sau o organizație internațională
    - posibilitatea, dacă este cazul, de a se opune prelucrării datelor lor, în condițiile prevăzute de articolul 21 din RGPD
    - condițiile și mijloacele puse la dispoziția persoanei vizate pentru a-și exercita, prin intermediul operatorului, drepturile de acces, rectificare și ștergere a datelor sale

- Atunci când este necesar și în vederea asigurării unei prelucrări corecte și transparente, informațiile trebuie să includă, de asemenea:
    - posibilitatea ca datele lor să fie prelucrate ulterior într-un scop compatibil, în conformitate cu garanțiile corespunzătoare prevăzute de lege și în conformitate cu condițiile prevăzute la articolul 5 alin.1 lit.b) din RGPD
    - posibilitatea de a depune o plângere la o autoritate de supraveghere
    - existența deciziilor automatizate, inclusiv crearea de profiluri, care este permisă numai în cazul în care este prevăzută de lege și sub rezerva unor garanții adecvate. Exemplu: identificarea, localizarea și monitorizarea unui pacient la distanță prin intermediul unor aplicații mobile și profilarea comportamentului acestuia. Orice decizie se ia în privința persoanei trebuie să aibă un factor uman în spate și să existe un control uman.

- Aceste informații ar trebui să fie furnizate **înainte de colectarea datelor sau la prima comunicare.**

- Informațiile trebuie să fie **inteligibile și ușor accesibile**, într-un limbaj clar și simplu și adaptate circumstanțelor, pentru a permite persoanei vizate să înțeleagă pe deplin prelucrarea prevăzută. În special, în cazul în care persoana vizată este incapabilă din punct de vedere fizic sau juridic să primească informațiile, acestea pot fi furnizate persoanei care o reprezintă legal. În cazul în care o persoană incapabilă din punct de vedere juridic este capabilă să înțeleagă, aceasta ar trebui, de asemenea, să fie informată înainte de prelucrarea datelor.

- Operatorul **nu este obligat să furnizeze aceste informații în cazul în care persoana vizată deține deja informațiile necesare.** În plus, în cazul în care datele cu caracter personal nu sunt colectate direct de la persoana vizată, operatorul nu este obligat să o informeze în cazul în care prelucrarea este prescrisă în mod expres de lege sau dacă acest lucru se dovedește a fi imposibil, de exemplu, în cazul în care datele de contact ale persoanei vizate s-au schimbat și aceasta nu poate fi găsită sau nu este accesibilă, sau dacă implică eforturi disproporționate din partea operatorului, în special în cazul prelucrării în scopuri de arhivare în interes public și în scopuri de cercetare științifică sau istorică sau în scopuri statistice.

- Dorința unei persoane de **a nu fi informată cu privire la un diagnostic sau la un prognostic** ar trebui respectată, cu excepția cazului în care acest lucru constituie un risc grav pentru sănătatea altor persoane.

- Operatorul **nu este obligat să informeze persoana vizată în cazul în care acest lucru este prevăzut de lege** și este necesar și proporțional într-o societate democratică, din motivele specificate expres de lege.

B. Drepturi care asigură controlul persoanei vizate asupra legalității și calității prelucrărilor de date: accesul la date, rectificarea, ștergerea, opoziția la prelucrare și portabilitatea datelor

- Persoana vizată are dreptul de a ști dacă datele cu caracter personal care o privesc sunt prelucrate și, în caz afirmativ, de a obține - fără întârzieri sau cheltuieli excesive și într-o formă inteligibilă - comunicarea datelor sale și de a avea acces, în aceleași condiții, cel puțin la următoarele informații:
    - scopul sau scopurile prelucrării
    - categoriile de date cu caracter personal în cauză
    - destinatarii sau categoriile de destinatari ai datelor și transferurile de date preconizate către o țară terță sau o organizație internațională
    - perioada de păstrare
    - raționamentul care stă la baza prelucrării datelor atunci când rezultatele unei astfel de prelucrări le sunt aplicate, în special în cazul creării de profiluri

- Persoana vizată (pacientul spre exemplu) are dreptul la **ștergerea datelor prelucrate** cu încălcarea legislației de protecție a datelor cu caracter personal, în special a RGPD

- Persoana vizată (pacient sau aparținător) are dreptul de a obține **rectificarea datelor** care o privesc. De asemenea, persoana vizată are dreptul de a se opune, din motive legate de situația sa personală, prelucrării datelor sale privind sănătatea, cu excepția cazului în care acestea sunt anonimizate sau dacă operatorul demonstrează un motiv imperios și legitim pentru continuarea prelucrării datelor.

- În cazul în care cererea de rectificare sau de ștergere a datelor este refuzată sau în cazul în care obiecția persoanei vizate este respinsă, aceasta are la dispoziție o **cale de atac.**

- Persoana vizată are dreptul de **a nu face obiectul unei decizii** care să o afecteze în mod semnificativ și care să se bazeze exclusiv pe prelucrarea automatizată, inclusiv crearea de profiluri, a datelor sale referitoare la sănătate. O derogare de la această interdicție ar fi posibilă numai în cazul în care o astfel de prelucrare se bazează pe consimțământul persoanei vizate sau este necesară din motive de interes public substanțial. Măsurile prevăzute de lege ar trebuie să fie proporționale cu scopul urmărit, să respecte esența dreptului la protecția datelor și să prevadă garanții adecvate și specifice pentru a proteja drepturile și libertățile fundamentale ale persoanei vizate.

- În cazul în care prelucrarea este efectuată prin mijloace automate, persoana vizată ar trebui să poată obține de la operator, în condițiile prevăzute de lege, **punerea la dispoziție** - într-un format structurat, interoperabil și ușor de citit automat - a datelor sale cu caracter personal în vederea **transmiterii acestora către un alt operator** (portabilitatea datelor). De asemenea, persoana vizată ar trebui să poată solicita operatorului să transmită datele direct unui alt operator.

- Profesioniștii din domeniul sănătății trebuie să pună în aplicare toate măsurile necesare pentru a asigura respectarea exercitării efective a acestor drepturi **ca parte a eticii lor profesionale.**

- Drepturile persoanei vizate **pot face obiectul unor restricții** în cazul în care aceste restricții sunt prevăzute de lege și reprezintă măsuri necesare și proporționale într-o societate democratică, în conformitate cu **articolul 23 din RGPD.**

- Legea trebuie să prevadă **garanții adecvate** care să asigure respectarea drepturilor persoanei vizate.

4.6 CONSIMȚĂMÂNTUL PERSOANELOR

SURSELE PRINCIPALE ALE NECESITĂȚII EXISTENȚEI CONSIMȚĂMÂNTULUI

Sursele principale ale necesității existenței unui Consimțământ la momentul desfășurării unor activități medicale de prevenție, diagnostic sau tratament sunt:

- **reglementările naționale:**
  - Legea 95/2006 privind reforma în domeniul sănătății
  - Legea nr. 46/2003 privind drepturile pacientului
  - Normele metodologice de aplicare a Legii 95/2006
  - alte acte normative specifice domeniului medical – se va ține cont de variantele la zi ale acestor acte normative
- **reglementări ale Uniunii Europene:**
  - Regulamentul General privind Protecția Datelor
  - Orientările nr. 05/2020 privind consimțământul în temeiul Regulamentului 2016/679 adoptate de Comitetul European pentru Protecția Datelor
  - alte acte normative și recomandări, ghiduri sau orientări specifice sectorului medical sau protecției datelor
- **reglementări internaționale**, cum este cazul Convenției de la Oviedo pentru protecția drepturilor omului și a demnității ființei umane față de aplicațiile biologiei și medicinei (1997)

Notă: Toate reglementările menționate anterior pretind într-un anumit context existența unui consimțământ, însă obiectivele categoriilor de normative uneori diferă, astfel că trebuie să se înțeleagă clar că în privința consimțământului nu se suprapun în totalitate. De aici, consecința este că procedura de obținere a consimțământului trebuie să integreze toate obiectivele, răspunzând tuturor necesităților și criteriilor impuse de categoriile principale de acte normative: necesități medicale, etice și de confidențialitate și protecție a datelor medicale.

CONSIMȚĂMÂNTUL, pentru motivele expuse mai sus, trebuie să fie luat pe mai multe nivele.

A. Primul nivel este cel pretins de Legea nr. 95/2006, la Capitolul III (articolele 660-662). Acest capitol poartă denumirea **”Acordul pacientului informat”**. Legea 95/2006 și Normele metodologice din 2007, de aplicare a titlului XVI din lege, cu modificările ulterioare, stabilesc **informațiile minime obligatorii** care vor fi cuprinse în documentul de Acord:

- diagnosticul
- natura și scopul tratamentului
- riscurile și consecințele tratamentului propus
- alternativele viabile de tratament, riscurile și consecințele lor
- prognosticul bolii fără aplicarea tratamentului

Acordul pacientului informat este dovedit și documentat prin completarea formularului de exprimare a acordului pacientului informat, formularul fiind prevăzut de Anexa 1 la Normele Metodologice.

Primul nivel de obținere a consimțământului este cel mai important, deoarece *obiectivele principale* ale obținerii acestuia sunt *Medicale*. Cu toate acestea, în mod *inerent* acordul cuprinde și informațiile solicitate pentru prelucrarea datelor medicale cu **scopul** prevenției, al diagnosticării sau acordării tratamentului medical. Din acest motiv, *funcția specifică* prelucrării datelor medicale cu scopul amintit este protejarea drepturilor și libertăților pacientului, în special a vieții, integrității fizice și psihice și a vieții sale private.

Extrem de Important: ”Acordul pacientului informat” Nu cuprinde un consimțământ în sensul articolului 9 alin.(2) lit. a) din Regulamentul General privind Protecția Datelor.

Acesta cuprinde un consimțământ de Informare cu privire la prelucrarea datelor medicale în scopurile amintite, însă această prelucrare are ca temei **articolul 9 alin.(2) litera h)**: *prelucrarea este necesară în scopuri legate de medicina preventivă sau a muncii, de evaluarea capacității de muncă a angajatului, de stabilirea unui diagnostic medical, de furnizarea de asistență medicală sau socială sau a unui tratament medical sau de gestionarea sistemelor și serviciilor de sănătate sau de asistență socială, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul unui contract încheiat cu un cadru medical și sub rezerva respectării condițiilor și garanțiilor prevăzute la alineatul (3).*

Concluzie: Prelucrarea datelor medicale la care face referire Legea 95/2006, menționate în **Formularul de exprimare a acordului pacientului informat**, are ca temei Legea, din perspectiva protecției datelor personale, iar nu consimțământul propriu-zis al pacientului. Consimțământul prevăzut de Legea 95/2006 va fi necesar doar pentru ca pacientul să beneficieze propriu-zis de serviciile medicale concrete la care apelează.

Existând această suprapunere, cu funcții diferite, apreciem că pentru ca Formularul de exprimare a consimțământului să îndeplinească cât mai eficient și standardele de protecție a datelor și să crească gradul său de conformare cu actul medical, se poate modifica în sensul completării sale, ori se poate utiliza un formular distinct prin care să se realizeze informarea pacienților și, dacă este cazul, a reprezentanților legali sau unor rude apropiate, conform legii.

Modificări asemănătoare, pentru rațiuni asemănătoare, se pot realiza în legătură cu **Formularul din Anexa nr. 2 privind raportul scris asupra asistenței medicale acordate în situații de urgență**, caz în care prelucrarea datelor cu caracter personal se realizează pe baza unui alt temei juridic, anume **articolul 9 alin. 2) lit c din Regulamentul General privind Protecția Datelor:** *prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice, atunci când persoana vizată se află în incapacitate fizică sau juridică de a-și da consimțământul.*

Completările formularelor din Anexa 1 și 2 au în vedere următoarele:

- completarea unor rubrici, pentru a avea un grad de concretețe mai mare: spre exemplu, la rubrica 5 intitulată **„Consimțământ pentru recoltare”**, în caseta 2 de pe același rând este menționat: *„Pacientul este de acord cu recoltarea, păstrarea și folosirea produselor biologice”*; se impune completarea astfel încât să rezulte un consimțământ pentru toate acele operațiuni sau doar pentru unele, în conformitate cu legea;

- la rubrica 6 intitulată **„Alte informații care au fost furnizate pacientului”** se va adăuga o casetă distinctă, denumită Informații privind prelucrarea datelor cu caracter personal în scopuri de prevenție, diagnosticare sau tratament potrivit Notei de Informare. Această Notă va cuprinde detaliat toate categoriile de prelucrări, temeiul legal, destinatarii datelor, drepturi specifice persoanei vizate în conformitate cu legislația privind protecția datelor, restricții specifice de prelucrare în absența unui consimțământ explicit.

- introducerea unei noi casete la rubrica 6 sau o nouă rubrică cu nr. 8, care să cuprindă **„Alte informații solicitate de către pacient”**

Acest proiect de formular îmbină primul nivel de reglementare a consimțământului cu cel de-al doilea nivel, care privește conformitatea cu Regulamentul General privind Protecția Datelor, iar nu obținerea unui consimțământ de prelucrare a datelor ci documentarea unei informări în acest sens.

Recomandare: Informațiile cuprinse în Acordul pacientului informat trebuie transmise cu o diligență asemănătoare cu cea existentă la acordarea propriu-zisă a actului medical, deoarece etica actului medical și reglementările aferente domeniului tratează această informare și acordul ulterior ca o componentă a actului medical propriu-zis, deoarece în ambele cazuri, consecințele directe se produc la nivel psihologic și determină și consecințe la nivel fizic și psihologic.

B. Al doilea nivel privește consimțământul obținut în scopul realizării unor prelucrări de date cu caracter personal, altele decât cele de prevenție, diagnosticare sau tratament acordat pacientului sau prelucrările de date obligatorii potrivit legii.

Acest consimțământ este specific Regulamentului General privind Protecția Datelor, prelucrarea datelor fiind întemeiată pe **articolul 9 alin. 2) litera a** coroborată cu unele dispoziții din RGPD, care sunt aplicabile în funcție de scopul concret al prelucrării, cum ar fi: cercetare științifică, scopuri didactice, statistice, de marketing etc.

Acesta este un document care trebuie realizat cu o acuratețe și grijă extrem de clară, deoarece nu poate condiționa în nici un fel efectuarea actului medical de furnizarea consimțământului de către pacient.

De aceea, atunci când este posibil, acest consimțământ se va obține numai după efectuarea activității medicale. În mod excepțional, atunci când o activitate accesorie actului medical este complet dependentă de participarea directă la momentul desfășurării acestuia, cum este cazul **vizualizării unei operații chirurgicale de către un grup de studenți**, consimțământul va fi solicitat în condiții specifice explicându-se cu o claritate foarte mare că nu are vreo influență asupra calității actului medical sau a furnizării acestuia.

Consimțământul trebuie obținut pentru fiecare scop în parte, pentru că trebuie să fie specific. Recomandăm cu fermitate ca un asemenea consimțământ să fie căutat doar când pacientul nu este influențat de diagnosticul prescris, de tratamentul acordat sau de starea în care se află. Un prim pas, poate fi parcurs astfel, oferindu-i-se pacientului o informare, pe care este rugat să o citească când are timp.

Informarea trebuie să fie simplă și succintă, arătându-i-se inițial că protecția sa presupune și o protecție a datelor sale, pe care poate sau nu să le furnizeze, în scopuri precum cele care vor fi enumerate. Ulterior, informarea poate să cuprindă următoarea exprimare: *dacă doriți să consimțiți ca datele dvs să fie prelucrate și în acest scop, vă rugăm să luați legătura cu _____ prin următoarea modalitate____*

În final, dacă se parcurge această etapă, se va trece la încheierea acordului de prelucrare a datelor, care trebuie să conțină toate elementele specifice GDPR și la momentul imediat anterior încheierii acestuia se va reveni asupra întregii dimensiuni și consecințe ale acestuia din perspectiva protecției datelor cu caracter personal.

Recomandare: Consimțământul avut în vedere la această secțiune are o preponderență în special la nivelul conformării operatorului de date cu întreaga legislație a protecției datelor. Cu toate acestea, un profesionist din domeniul sănătății va căuta crearea unei legături reale și motivaționale cu persoana vizată, evitând să trateze problema doar ca un formalism prevăzut de lege. În realitate, acest formalism acoperă probleme de etică, de malpraxis și de răspundere juridică.

PAȘII ESENȚIALI ÎN REALIZAREA CONSIMȚĂMÂNTULUI ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL

A. Datele care trebuie avute în vedere în mod obișnuit

În activitățile medicale, farmaceutice și accesorii acestor activități sunt vehiculate date ale pacienților sau date ale persoanelor care îi tutoriază, acestea reprezentând categoriile curente de date și fluxuri. În cele ce urmează vor fi reprezentate **cele mai uzuale categorii de date și fluxuri:**

- note scrise de mână, consemnate sub forma rețetelor medicale
- înregistrări electronice, în special în dosarele electronice de sănătate și în registrele proprii ale operatorului
- comunicări verbale, pe suport de hârtie sau electronice între profesioniștii din domeniul sănătății, cu scop de consultare, diagnosticare sau prevenție
- înregistrări vizuale și audio, cu scop de analiză, pregătire ante-operatorie, cercetare științifică etc.
- rapoarte de laborator, privind analize
- dialogul cu pacienții, sub orice formă: verbal, electronic sau pe suport de hârtie

Notă: Conștientizați fluxurile precizate mai sus, deoarece acestea pun în discuție date cu caracter personal, iar protecția lor juridică este activă, prin legislația care protejează viața privată, incluzând dreptul la confidențialitate al persoanei vizate sau prin legislația specifică de protecție a datelor personale, în esență prevederile Regulamentului General de Protecție a Datelor

Rele practici: Majoritatea se bazează pe un comportament neintenționat, dar lipsit de conștientizare pe linia de protecție a datelor! **Exemple:**

- Comunicarea în zone publice, între medic/asistent și pacient (pe holul unității sanitare, medicul iese grăbit și își cheamă unul dintre pacienți: Să vină cel care are dureri de stomac!)
- Consemnările pe hârtie afișate la patul pacienților internați în încăperi cu mai multe paturi și pacienți, în care accesul altor persoane nu este controlat (există riscul dezvăluirii unor date medicale către persoane neautorizate sau riscul pierderii consemnărilor!)

B. Orice activitate desfășurați, uitați-vă dacă mai este necesară colectarea datelor sau prelucrarea lor, ori uitați-vă dacă este suficientă prelucrarea anonimizată a datelor, raportat la scop

Iată un **exemplu**:

- Să presupunem că medicul tratează un pacient cu o formă rară de cancer. Medicul dorește să obțină sfaturi sau informații suplimentare de la colegi sau experți în domeniu pentru a se asigura că aplică cel mai bun tratament posibil.
- În acest caz, medicul poate să transmită informații anonimizate despre pacient și boala acestuia, fără a dezvălui identitatea pacientului. Anonimizarea se face prin eliminarea oricăror date care ar putea identifica direct sau indirect pacientul, cum ar fi numele, adresa, CNP, numărul de telefon, adresa de e-mail, fotografii etc.
- Medicul poate să prezinte cazul într-un format anonim, folosind informații precum vârsta, sexul, simptomele, istoricul medical și rezultatele testelor, fără a include detalii care ar putea identifica pacientul. Astfel, se asigură protecția confidențialității pacientului și respectarea legilor privind protecția datelor cu caracter personal, în timp ce beneficiază de expertiza altor profesioniști din domeniul medical pentru a oferi cel mai bun tratament pacientului.

Notă: Țineți cont că majoritatea datelor medicale transmise fără identificarea pacientului nu pot fi corelate ușor, iar GDPR protejează această chestiune. Excepție: unitatea medicală are un soft care prelucrează automat informațiile biologice, de ADN, și le corelează cu identitatea unei persoane! Cu toate acestea, în majoritatea cazurilor, fotografiile sau transmiterea acestora lipsite de identificare nominală nu sunt contrare GDPR!

C. Protejați informațiile personale astfel încât să aveți sentimentul de control complet asupra gestiunii acestora, iar accesul neautorizat și lipsit de interes profesional să fie împiedicat, inclusiv divulgarea de alții sau pierderea unor informații să fie excluse.

Iată un **exemplu**:

- Majoritatea unităților medicale utilizează sisteme informatice pentru înregistrarea datelor colectate de la pacienți și cu privire la pacienți. Înainte de a utiliza orice dispozitive informatice, precum telefoane mobile, laptopuri etc., este obligatoriu ca sistemul să fie implementat și verificat, inclusiv întreținut de specialiști care acreditează concret securitatea și viabilitatea sistemului. Răspunderea revine unității medicale, însă utilizarea și observarea curentă a sistemului se realizează prin personalul medical și administrativ al unității, astfel că orice neregulă care apare trebuie imediat sesizată și raportată managementului.

Notă: Una dintre cele mai des întâlnite greșeli este absența raportării diferitelor disfuncționalități care apar în linia administrativă de utilizare și încărcare, transmitere a datelor în sistemele informatice sau în transmiterea pe suport de hârtie a unor informații cu caracter personal.

Această disfuncționalitate se datorează unei încrederi lipsite de fundament, că toate disfuncționalitățile se gestionează de management, iar personalul medical trebuie să se implice exclusiv în actul medical. Recomandarea noastră este să notați orice mică disfuncționalitate privind protecția datelor și să o raportați verbal sau în scris managementului sau persoanei cu atribuții specifice în protecția datelor cu caracter personal.

D. Fiți conștienți de responsabilitățile dumneavoastră prin raportare la rolul pe care îl aveți în organizație.

Rolurile într-o organizație sunt diferențiate pe categorii, chiar și acolo unde este funcțional, spre exemplu, un cabinet de stomatologie cu doi angajați. Partajarea datelor personale sau orice activitate care presupune utilizarea de date personale nu trebuie efectuată pe toate nivelele de ambii angajați.

Este o chestiune de management organizațional ca fiecăruia să i se stabilească de la început și să i se explice ce nivel de cunoaștere poate avea asupra informațiilor care se prelucrează și cum anume are guvernanța datelor la care poate avea acces.

Aceste aspecte manageriale sunt stabilite în funcție de necesitatea de a cunoaște anumite informații, necesitate care îi permite și utilizarea acestora potrivit acelor necesități.

Notă: Luați în considerare că această conștientizare a responsabilităților trebuie obligatoriu realizată în contextul raporturilor de muncă cu angajatorul, motiv pentru care trebuie să fiți atenți ca la începutul relației de muncă să solicitați o instruire în acest sens, pe care ar fi recomandat să o și documentați.

E. Utilizați la începutul relației cu pacientul Formularul de consimțământ al pacientului informat prevăzut de Normele de aplicare ale Legii privind reforma în domeniul sănătății, completat potrivit recomandărilor din acest ghid.

Recomandăm cu fermitate ca această activitate să fie realizată cu grijă, conștientizată și contextualizată: **Nu se va trata cu superficialitate sau ca o formalitate!**

Se va realiza într-un context familiar, explicându-i-se pacientului că tratamentul pe care s-ar putea să îl urmeze și relația cu unitatea medicală, dar mai ales cu medicul, necesită utilizarea unor date private și o legătură extrem de familiară între medic și pacient!

Nu se va utiliza și completa formularul **sub presiunea tratamentului** sau a îngrijirilor medicale! În funcție de acest context personalizat transmiterea verbală a informațiilor din formular se va face într-o formă mai succintă sau mai detaliată, evidențiindu-se verbal aspectele relevante!

Pacientul va fi informat că **îngrijirea sa este o datorie esențială a medicilor**, motiv pentru care toate **datele sale vor fi protejate de lege**, fiind confidențiale și sunt strict prelucrate potrivit legii! Aici, se poate face referire la **nota de informare** cu privire la prelucrările de date din cadrul unității, care i-a fost adusă la cunoștință, în mod obișnuit, la momentul primirii în unitatea medicală, notă care prevede că unitatea medicală prelucrează următoarele categorii de date:

- date în legătură cu tratamentul acordat direct
- date de audit din cadrul instituției, potrivit principiilor de protecție a datelor
- date pe care legea le pretinde
- dacă este cazul, date prelucrate în scop de interes public

Pacientul este informat că sunt prelucrate și alte date, dar necesită un consimțământ special, avut în vedere la litera F.

F. Pacientul este informat că unitatea medicală poate prelucra și alte date, dar cu consimțământul explicit la pacientului.

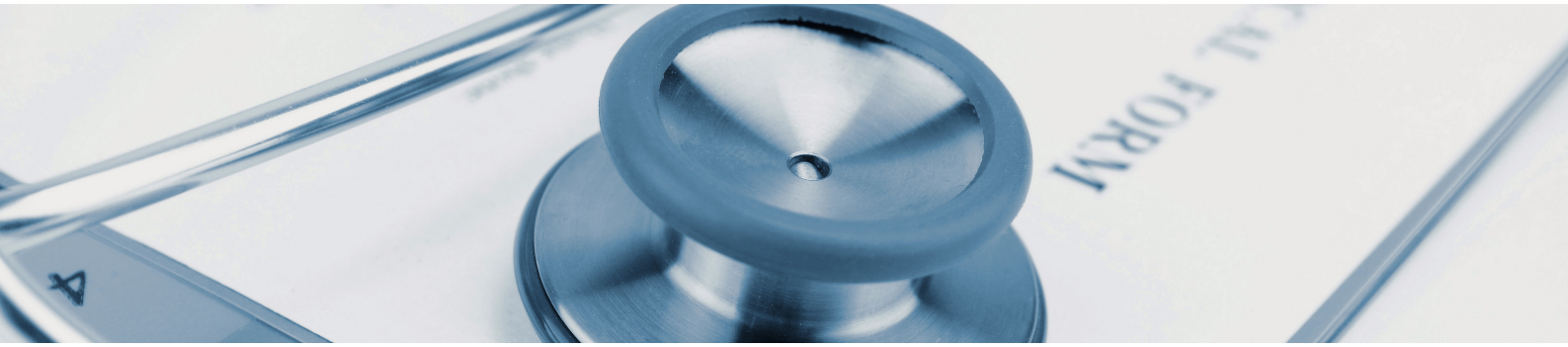
Acesta este pasul care se aplică doar dacă prelucrările de date se realizează în alte scopuri decât cele de la litera D, adică cele prevăzute în formularul de consimțământ, prevăzut de Normele metodologice ale Legii privind reforma în domeniul sănătății!

Recomandăm, dacă este posibil, să fie luat doar **după acordarea tratamentului**, în special dacă **scopul prelucrării este de marketing**!

Pacientul este informat că numai acceptul său poate permite o asemenea prelucrare!

Notă finală:
Faceți distincția între următoarele concepte:

- **Notă de informare** cu privire la prelucrările de date
  - conține date obligatoriu de furnizat indiferent că pacientul urmează sau nu un tratament
  - se face la începutul relației cu un posibil pacient
  - poate fi realizată direct de către personalul administrativ al unității medicale
  - conține date care se pot regăsi în unele rubrici ale Formularului privind consimțământul pacientului informat
  - este cerută în special de RGPD
- **Formular de consimțământ al pacientului informat**, prevăzut de Legea privind reforma în domeniul sănătății (recomandat, cu completările presupuse de acest ghid)
  - nu este un consimțământ propriu-zis al pacientului privind prelucrarea datelor cu caracter personal
  - este cerut de Legea națională privind reforma în domeniul sănătății
  - este o garanție deopotrivă a eticii în domeniul medical și este un consimțământ al pacientului de a urma un tratament
  - cuprinde și unele date la care face referire nota de informare, însă de regulă mult mai detaliate
  - prelucrarea datelor la care se face referire în Formular se poate realiza indiferent că pacientul este sau nu de acord cu această prelucrare
- **Consimțământul necesar pentru prelucrarea datelor**
  - nu este dependent de cauzele pentru care se face prelucrarea datelor prevăzute în Formular
  - este obligatoriu, dacă prelucrarea nu vizează acordarea directă a tratamentului, prelucrarea obligatorie prevăzută de lege (inclusiv pentru protejarea unui interes vital al pacientului) sau prelucrarea în interes public
  - se documentează pe un formular distinct



PARTEA a IV-a | CAPITOLUL 5

RESURSE UTILE

Legislație | Formulare | Ghiduri | Recomandări
Bibliografie | Studii de caz | Resurse adiționale

GHID DEZVOLTAT DE

ÎN COLABORARE CU GDPRComplet.ro

În **Partea a IV-a** a acestui ghid vom aborda aspectele practice ale conformității cu GDPR în cadrul sistemului medical românesc, prin prezentarea unor materiale și resurse utile, care pot facilita înțelegerea și aplicarea eficientă a reglementărilor privind protecția datelor. Scopul acestei secțiuni este de a pune la dispoziția medicilor, personalului medical și celor implicați în domeniul sănătății, instrumente concrete care să îi ajute în procesul de asigurare a protecției datelor cu caracter personal.

Această parte a ghidului cuprinde:

- **Legislația relevantă**: acte normative și reglementări naționale și internaționale care au impact asupra protecției datelor în sistemul medical, pentru a facilita accesul la informații și a oferi un punct de plecare în înțelegerea cadrului legislativ.

- **Formulare și șabloane**: exemple de formulare și șabloane care pot fi utilizate în diverse situații, precum obținerea consimțământului, gestionarea cererilor persoanelor vizate sau raportarea încălcărilor de securitate. Aceste documente pot fi adaptate și personalizate în funcție de nevoile specifice ale fiecărei unități medicale.

- **Ghiduri și recomandări ale autorităților de protecție a datelor:** o selecție de materiale publicate de autoritățile de protecție a datelor din România și din Uniunea Europeană, care pot fi utile în procesul de conformare la GDPR. Aceste materiale includ orientări, recomandări și exemple de bune practici.

- **Studii de caz și exemple**: studii de caz și exemple relevante care ilustrează modul în care principiile și reglementările privind protecția datelor au fost aplicate în contextul medical, precum și consecințele nerespectării acestor prevederi.

- **Resurse adiționale**: linkuri către articole, publicații și materiale educaționale, care pot contribui la aprofundarea cunoștințelor și la înțelegerea mai bună a aspectelor legate de protecția datelor în sistemul medical.

Legislație relevantă

- Elementul principal de legislație la care am făcut referință este: Regulamentul nr. 679 din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (**Regulamentul general privind protecţia datelor**): *https://www.dataprotection.ro/servlet/ViewDocument?id=1262*

- În completarea R.G.P.D., pe website-ul ANSPDCP mai puteți găsi și alte norme legislative relevante: *https://www.dataprotection.ro/?page=legislatie_comunitara&lang=ro*

- Legea drepturilor pacientului

- Contractul cadru și normele metodologice de aplicare a contractului cadru

Formulare și șabloane

- **Anexa 1 -** Model de clauze care ar trebui luate în relație cu angajații

- **Anexa 2 -** Model de acord de confidențialitate pe care să îl utilizați în relație cu colaboratorii persoane împuternicite

- **Anexa 3 -** Tabel centralizator urmarire monitorizare

- **Anexa 4 -** Consimțământ specific RGPD

- **Anexa 5 -** Formularul tip cerere de acces la datele cu caracter personal

- **Anexa 6 -** Model de procedură de soluționare a cererilor persoanei vizate

- **Anexa 7 -** Model de formular de răspuns la cererile persoanei vizate

- **Anexa 8 -** Procedură privind managementul incidentelor de securitate

Ghiduri și recomandări ale autorităților de protecție a datelor

Iată o listă a ghidurilor, recomandărilor și orientărilor specifice emise de Grupul de lucru Articolul 29 (WP29) și Comitetul European pentru Protecția Datelor (EDPB):

- Ghid privind consimțământul în conformitate cu GDPR (WP259)
- Ghid privind transparența în conformitate cu GDPR (WP260)
- Ghid privind notificarea încălcărilor de securitate a datelor (WP250)
- Ghid privind impactul asupra protecției datelor și evaluarea riscurilor (DPIA) (WP248)
- Ghid privind responsabilul cu protecția datelor (DPO) (WP243)
- Ghid privind dreptul la portabilitatea datelor (WP242)
- Ghid privind profilarea și decizia individuală automată (WP251)
- Ghid privind transferurile internaționale de date în temeiul GDPR (WP244)
- Ghid privind utilizarea cookie-urilor și a altor tehnologii de urmărire (WP44)
- Ghid privind procesorii și subcontractorii în conformitate cu GDPR (WP282)
- Ghid privind certificarea în conformitate cu GDPR (WP261)
- Ghid privind codurile de conduită în conformitate cu GDPR (WP29)
- Ghid privind temeiul juridic pentru prelucrarea datelor cu caracter personal în cadrul prevenirii, detectării, investigării și persecutării infracțiunilor sau executării sancțiunilor penale (WP29)
- Ghid privind dreptul la ștergerea datelor ("dreptul de a fi uitat") (WP29)

Mai multe informații puteți găsi accesând linkul de mai jos:
https://edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines_ro?page=0

Literatură de specialitate în domeniul protecției datelor

- The protection of personal data in health information systems – principles and processes for public health. Copenhagen: WHO Regional Office for Europe; 2020. License: CC BY-NC-SA 3.0 IGO.
- Guide to Privacy and Security of Electronic Health Information, Version 2.0.,The Office of the National Coordinator for Health Information Technology, 2015

- Guidelines on Privacy in the Private Health Sector, Office of the Federal Privacy Commissioner, 2001
- Privacy Toolkit, A guide for physical therapists, College of Physical Therapists of British Columbia, 2020
- Confidentiality: good practice in handling patient information, General Medical Council, 2017.
- Manual de legislație europeană privind protecția datelor, Agenția pentru Drepturi Fundamentale a Uniunii Europene/Consiliul Europei, 2014

Rapoarte de activitate ale Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal:

- Raport de activitate A.N.S.P.D.C.P., 2006, București
- Raport de activitate A.N.S.P.D.C.P., 2007, București
- Raport de activitate A.N.S.P.D.C.P., 2008, București
- Raport de activitate A.N.S.P.D.C.P., 2009, București
- Raport de activitate A.N.S.P.D.C.P., 2010, București
- Raport de activitate A.N.S.P.D.C.P., 2011, București
- Raport de activitate A.N.S.P.D.C.P., 2012, București
- Raport de activitate A.N.S.P.D.C.P., 2013, București
- Raport de activitate A.N.S.P.D.C.P., 2014, București
- Raport de activitate A.N.S.P.D.C.P., 2015, București
- Raport de activitate A.N.S.P.D.C.P., 2016, București
- Raport de activitate A.N.S.P.D.C.P., 2017, București
- Raport de activitate A.N.S.P.D.C.P., 2018, București
- Raport de activitate A.N.S.P.D.C.P., 2019, București
- Raport de activitate A.N.S.P.D.C.P., 2020, București
- Raport de activitate A.N.S.P.D.C.P., 2021, București

Studii de caz și exemple. Cauze CEDO cu privire la datele medicale

- **Yvonne Chave împotriva Franței (64915/01)**
  - Reclamanta s-a plâns de accesul la dosarul ei medical privind internarea într-un spital psihiatric
  - Cererea a fost declarată inadmisibilă (în mod vădit nefondată)
  - CEDO a apreciat că dosarul era protejat de reguli de confidențialitate și acces adecvat

- **Gillberg împotriva Suediei (41723/06)**
  - Reclamantul, un profesor, a fost condamnat penal pentru refuzul de a permite accesul la cercetări privind hiperactivitatea și deficitul de atenție la copii
  - CEDO a decis că articolul 8 și articolul 10 nu se aplică în acest caz
  - Profesorul nu poate invoca dreptul la viața privată sau un drept „negativ” la libertatea de exprimare în acest context

- **Frâncu împotriva României (57129/10)**
  - Reclamantul s-a plâns de încălcarea dreptului la respectarea vieții private în urma respingerii cererii de ședință închisă într-o procedură referitoare la detenția sa provizorie
  - CEDO a constatat o încălcare a articolului 8, deoarece instanța de apel nu a asigurat confidențialitatea informațiilor medicale despre reclamant
  - Curtea a considerat că instanța de apel nu a realizat o evaluare proporțională și individualizată a cererii de ședință închisă

- **Järvinen împotriva Finlandei (45123/98)**
  - Reclamantul s-a plâns de divulgarea neautorizată a informațiilor medicale într-un raport de expertiză medico-legală
  - CEDO a constatat o încălcare a articolului 8, deoarece Finlanda nu a reușit să îndeplinească obligațiile pozitive pentru a proteja informațiile medicale ale reclamantului
  - Curtea a considerat că statul are datoria de a adopta măsuri eficiente pentru a proteja confidențialitatea informațiilor medicale

- **M.S. împotriva Croației (36337/10)**
  - Reclamanta s-a plâns de lipsa confidențialității în cazul unei acțiuni civile în care a fost acuzată de agresiune
  - CEDO a constatat o încălcare a articolului 8, deoarece instanțele croate nu au acordat importanță confidențialității informațiilor medicale ale reclamantei
  - Curtea a apreciat că instanțele ar fi trebuit să ia măsuri pentru a proteja confidențialitatea informațiilor medicale în contextul procedurilor judiciare

- **L.H. împotriva Letoniei (52019/07)**
  - Cazul se referă la o femeie care a contestat faptul că informațiile medicale personale legate de tratamentul ei pentru infertilitate au fost dezvăluite publicului și au fost utilizate într-un proces penal împotriva ei.
  - Reclamanta a susținut că dezvăluirea și utilizarea acestor informații au încălcat dreptul său la respectarea vieții private și de familie.
  - Soluția CEDO: Curtea a decis că a existat o încălcare a articolului 8 al Convenției și a acordat despăgubiri reclamantei.

- **Z. împotriva Finlandei (22009/93)**
  - Reclamanta s-a plâns de divulgarea neautorizată a statutului său de persoană infectată cu HIV în cadrul unor proceduri judiciare împotriva soțului său.
  - CEDO a constatat o încălcare a articolului 8, deoarece Finlanda nu a reușit să protejeze confidențialitatea informațiilor medicale ale reclamantei
  - Curtea a considerat că protecția confidențialității informațiilor medicale este esențială pentru respectarea dreptului la viața privată

- **L.L. împotriva Franței (7508/02)**
  - Reclamantul se plângea în special de prezentarea în fața instanțelor și utilizarea de către acestea a unor documente din dosarul său medical, în contextul unei proceduri de divorț, fără consimțământul său și fără desemnarea unui expert medical în acest sens.
  - Curtea a constatat o încălcare a articolului 8 al Convenției (dreptul la respectarea vieții private și de familie) și a acordat despăgubiri reclamantului.

- **Chave născută Jullien împotriva Franței (19131/07)**
    - Reclamanta a contestat păstrarea dosarului, într-o evidență centralizată, privind internarea sa obligatorie într-un spital psihiatric, internare considerată nelegală de instanțele franceze
    - CEDO a considerat că nu a existat o încălcare a dreptului la viața privată, deoarece Franța a luat măsuri adecvate pentru a reglementa accesul la datele personale și a înlătura orice riscuri nerezonabile

- **Vukota-Bojic împotriva Elveției (61838/10)**
    - Reclamanta a contestat supravegherea sa secretă de către detectivi angajați de asigurătorul său în urma unui accident rutier
    - CEDO a considerat că a existat o încălcare a dreptului la viața privată, deoarece supravegherea a fost intruzivă și a fost folosită în mod necorespunzător în procesul judiciar

- **M.E. împotriva Suediei (20837/92)**
    - Reclamanta a contestat comunicarea dosarelor medicale privind întreruperea de sarcină către un organism de asigurări sociale
    - CEDO a considerat că a existat o încălcare a dreptului la viața privată, deoarece divulgarea informațiilor sensibile nu a fost justificată

- **Armonas împotriva Lituaniei și Biriuk împotriva Lituaniei (47698/99)**
    - Reclamanții au contestat publicarea informațiilor despre starea lor de sănătate (fiind seropozitivi) într-un cotidian din Lituania. În 2001, cel mai mare cotidian din Lituania a publicat un articol pe prima pagină despre amenințarea SIDA într-o zonă îndepărtată din Lituania. În special, angajații dintr-un centru medical pentru combaterea SIDA și dintr-un spital erau citați drept confirmând că reclamanții erau seropozitivi. Despre cea de a doua reclamantă, descrisă ca fiind „renumită pentru promiscuitate”, se afirma că ar avea doi copii ilegitimi cu primul reclamant.
    - CEDO a considerat că a existat o încălcare a dreptului la viața privată, deoarece divulgarea informațiilor personale sensibile nu a fost justificată de interesele publice

- **Avilkina și alții împotriva Rusiei (1585/09)**
  - Reclamanții erau o organizație religioasă, Centrul Administrativ al Martorilor lui Iehova din Rusia și trei martori ai lui Iehova
  - Aceștia se plângeau în special despre divulgarea dosarelor lor medicale către autoritățile de urmărire penală ruse, în urma refuzului lor de a face transfuzii de sânge pe durata internării în spitale publice
  - CEDO a constatat o încălcare a dreptului la viața privată, deoarece divulgarea dosarelor medicale ale reclamanților autorităților penale nu a fost proporțională și a încălcat dreptul lor la respectarea vieții private

- **Radu împotriva Republicii Moldova (17475/05)**
  - Reclamanta, lector la Academia de Poliție, se plângea despre divulgarea de către un spital de stat de informații medicale despre ea către angajatorul său
  - Informațiile au circulat la scară largă la locul de muncă al reclamantei și, la puțin timp după aceasta, a pierdut sarcina din cauza stresului
  - CEDO a constatat o încălcare a dreptului la viața privată, deoarece divulgarea informațiilor medicale personale către angajator și diseminarea lor ulterioară au încălcat dreptul reclamantei la respectarea vieții private

- **Odièvre împotriva Franței (42326/98)**
  - Reclamanta s-a plâns că nu a putut obține detalii despre familia sa naturală, fiind abandonată la naștere și lăsată în grija serviciului pentru securitate și sănătate socială
  - CEDO a considerat că nu a existat o încălcare a dreptului la viața privată, deoarece Franța a avut un sistem adecvat de protecție a intereselor și drepturilor persoanelor implicate, inclusiv ale mamei naturale și ale copilului abandonat

- **Roche împotriva Regatului Unit (32555/96)**
  - Reclamantul s-a plâns că nu a avut acces la toate informațiile relevante și adecvate care să-i permită să evalueze eventualele riscuri la care a fost expus pe durata participării sale la testele cu gaz mușstar și gaz neurotoxic desfășurate sub auspiciile forțelor armate britanice în anii '60
  - CEDO a considerat că nu a existat o încălcare a dreptului la viața privată, deoarece Regatul Unit a oferit informații suficiente despre riscurile asociate testelor și a luat măsuri adecvate pentru a proteja sănătatea și siguranța participanților

- **Y.F. împotriva Turciei (17312/03)**
  - Reclamantul s-a plâns de dezvăluirea stării sale de sănătate (fiind seropozitiv) în timpul unei audieri în fața unei instanțe
  - CEDO a constatat o încălcare a dreptului la viața privată, deoarece divulgarea informațiilor medicale personale în public nu era necesară și nu exista un interes legitim care să justifice această încălcare

- **L. și V. împotriva Austriei (39392/98)**
  - Reclamanții s-au plâns de încălcarea dreptului la viața privată ca urmare a faptului că informațiile medicale personale ale acestora, inclusiv înregistrările video ale unor proceduri medicale, au fost prezentate în fața instanțelor într-un proces penal împotriva unui medic care i-a tratat
  - CEDO a constatat o încălcare a dreptului la viața privată, deoarece nu au fost luate măsuri suficiente pentru a proteja confidențialitatea datelor medicale ale reclamanților în cadrul procedurilor judiciare

- **K.H. și altele împotriva Slovaciei (32881/04)**
  - Reclamantele, opt femei de etnie romă, nu au mai putut rămâne însărcinate după ce au fost tratate la secțiile de ginecologie din două spitale diferite, acestea suspectând că fuseseră sterilizate în perioada spitalizării lor
  - Se plângeau că nu au putut obține fotocopii ale dosarelor lor medicale
  - CEDO a constatat o încălcare a dreptului la viața privată, deoarece reclamantele nu au avut acces la dosarele lor medicale, ceea ce a împiedicat exercitarea efectivă a dreptului lor la un recurs efectiv în legătură cu suspiciunile lor privind sterilizările forțate

- **Panteleyenko împotriva Ucrainei (11901/02)**
  - Reclamantul se plângea în special despre divulgarea, în cursul unei ședințe de judecată, de informații confidențiale despre starea sa psihică și tratamentul psihiatric pe care îl urma
  - CEDO a constatat o încălcare a dreptului la viața privată, deoarece divulgarea informațiilor medicale personale într-un cadru public nu a fost justificată și a încălcat dreptul reclamantului la respectarea vieții private

- **Anne-Marie Anderson împotriva Suediei (29870/96), 1997**
    - Reclamanta a fost diagnosticată cu cancer și și-a pierdut locul de muncă în timp ce era în concediu medical. Ea a solicitat să primească ajutor social și a trebuit să furnizeze informații medicale detaliate autorităților. Ulterior, un oficial al agenției de asistență socială a discutat cu alte persoane despre cazul reclamantei și starea sa de sănătate.
    - CEDO a constatat o încălcare a dreptului la viața privată, deoarece autoritățile suedeze nu au asigurat confidențialitatea informațiilor medicale ale reclamantei, iar divulgarile neautorizate au constituit o ingerință în viața sa privată.

- **Mockutė împotriva Lituaniei (66490/09)**
    - Reclamanta se plângea de lipsa de confidențialitate în ceea ce privește informațiile medicale din dosarul său, precum și faptul că întreruperea sarcinii sale a fost înregistrată în dosarul său medical fără consimțământul ei.
    - CEDO a constatat o încălcare a dreptului la viața privată, deoarece autoritățile lituaniene nu au protejat în mod adecvat confidențialitatea informațiilor medicale ale reclamantei și au înregistrat procedura de avort în dosarul ei medical fără consimțământul ei.

- **Konovalova împotriva Rusiei (37854/04)**
    - Reclamanta, o femeie însărcinată, a fost supusă unei cezariene în prezența mai multor studenți la medicină, fără să îi fi fost cerut consimțământul în prealabil. Ea susținea că dreptul ei la viață privată și demnitate personală a fost încălcat.
    - CEDO a constatat o încălcare a dreptului la viața privată, deoarece autoritățile ruse nu au obținut consimțământul reclamantei înainte de a permite studenților să asiste la intervenția chirurgicală.

- **Peck împotriva Regatului Unit (44647/98)**
    - Reclamantul a fost surprins de camerele de supraveghere în timp ce încerca să se sinucidă într-un loc public. Imaginile au fost ulterior difuzate în mass-media fără consimțământul său.
    - CEDO a constatat o încălcare a dreptului la viața privată, deoarece difuzarea imaginilor a constituit o ingerință în viața privată a reclamantului, iar autoritățile nu au oferit garanții suficiente pentru a proteja drepturile sale.

- **Malanicheva împotriva Rusiei (69414/01)**
    - Reclamanta, o pacientă seropozitivă, a fost internată în spital pentru tratament. Fără consimțământul ei, personalul spitalului a dezvăluit statutul ei HIV unor pacienți, iar aceștia au făcut informația publică.
    - CEDO a constatat o încălcare a dreptului la viața privată, deoarece statul rus nu a protejat confidențialitatea informațiilor medicale ale reclamantei și a permis divulgarea neautorizată a statutului ei HIV.

- **M.D. și alții împotriva Spaniei (67875/21)**
    - Reclamanții erau un grup de migranți care au fost depistați pozitivi la testul pentru boala COVID-19. Autoritățile spaniole au divulgat public identitatea acestora, ceea ce a condus la stigmatizarea și discriminarea lor în comunitatea locală.
    - CEDO a constatat o încălcare a dreptului la viața privată, deoarece autoritățile spaniole au divulgat informații medicale personale și sensibile despre reclamanți fără a obține consimțământul lor.

- **Kotilainen și alții împotriva Finlandei (62439/12)**
    - Reclamanții se plângeau de încălcarea dreptului la viața privată în urma unui atac cibernetic care a compromis datele lor personale și medicale stocate de o clinică privată de sănătate mintală
    - CEDO a constatat o încălcare a dreptului la viața privată, deoarece statul nu a reușit să protejeze în mod adecvat datele personale și medicale ale reclamanților în fața riscului unui atac cibernetic

- **Tysiąc împotriva Poloniei (5410/03)**
    - Cazul se referă la o femeie care suferea de o afecțiune oculară și care a rămas însărcinată. Medicii au avertizat-o că sarcina și nașterea ar putea agrava starea ochilor ei, dar nu i-au acordat avortul legal din motive terapeutice.
    - Reclamanta a susținut că autoritățile poloneze au încălcat dreptul său la respectarea vieții private, întrucât nu a avut acces la un avort legal și sigur, în ciuda riscurilor pentru sănătatea ei.
    - Soluția CEDO: Curtea a decis că a existat o încălcare a articolului 8 (dreptul la respectarea vieții private și de familie) al Convenției.

- **Szuluk împotriva Regatului Unit (36936/05)**
  - Cazul viza dreptul la confidențialitatea corespondenței dintre un deținut și medicii săi.
  - Reclamantul a afirmat că autoritățile penitenciare au încălcat dreptul său la respectarea vieții private prin monitorizarea și deschiderea corespondenței medicale.
  - Soluția CEDO: Curtea a decis că a existat o încălcare a articolului 8 al Convenției și a acordat despăgubiri reclamantului.

- **Léger împotriva Franței (19324/02)**
  - Cazul se referă la un bărbat care a fost contaminat cu HIV în urma unui tratament medical și a încercat să obțină informații despre sursa contaminării.
  - Reclamantul a susținut că autoritățile franceze nu au respectat dreptul său la respectarea vieții private și de familie, întrucât nu i-au permis să afle sursa contaminării cu HIV.
  - Soluția CEDO: Curtea a decis că nu a existat o încălcare a articolului 8 al Convenției.

- **P. și S. împotriva Poloniei (57375/08)**
  - Cazul se referă la o fată de 14 ani care a rămas însărcinată în urma unui viol și a întâmpinat dificultăți în accesarea unui avort legal.
  - Reclamanții au susținut că autoritățile poloneze au încălcat dreptul la respectarea vieții private și de familie prin refuzul de a le acorda accesul la un avort legal și prin divulgarea informațiilor medicale.
  - Soluția CEDO: Curtea a decis că au existat încălcări ale articolului 8 al Convenției și a acordat despăgubiri reclamanților.

- **Gaskin împotriva Regatului Unit (10454/83)**
  - Cazul se referă la un bărbat care a fost crescut în îngrijirea statului și care a solicitat accesul la dosarul său de asistență socială pentru a afla detalii despre copilăria și tratamentul său în timpul perioadei în care a fost în grija statului.
  - Reclamantul a susținut că refuzul autorităților de a-i permite accesul la dosarul său a încălcat dreptul său la respectarea vieții private și de familie.
  - Soluția CEDO: Curtea a decis că a existat o încălcare a articolului 8 al Convenției și a acordat despăgubiri reclamantului.

- **Juhnke împotriva Germaniei (52515/99)**
    - Cazul se referă la o femeie care a solicitat accesul la dosarul medical al mamei sale decedate pentru a afla dacă aceasta a avut vreo predispoziție genetică pentru cancer.
    - Reclamanta a susținut că refuzul autorităților germane de a-i acorda accesul la dosarul medical al mamei sale a încălcat dreptul său la respectarea vieții private.
    - Soluția CEDO: Curtea a decis că nu a existat o încălcare a articolului 8 al Convenției.

- **Trocellier împotriva Franței (29967/96)**
    - Cazul se referă la un bărbat a cărui soție a murit într-un spital, iar reclamantul a solicitat accesul la dosarul medical al soției sale pentru a determina cauza decesului.
    - Reclamantul a susținut că refuzul autorităților franceze de a-i permite accesul la dosarul medical al soției sale a încălcat dreptul său la respectarea vieții private și de familie.
    - Soluția CEDO: Curtea a decis că nu a existat o încălcare a articolului 8 al Convenției.

- **I. împotriva Finlandei (20511/03)**
    - Cazul se referă la o femeie care a descoperit că angajatorul său, un spital, a accesat în mod neautorizat dosarul său medical.
    - Reclamanta a susținut că autoritățile finlandeze nu au respectat dreptul său la respectarea vieții private și de familie prin nerespectarea confidențialității datelor medicale personale.
    - Soluția CEDO: Curtea a decis că a existat o încălcare a articolului 8 al Convenției și a acordat despăgubiri reclamantei.

- **B.B. împotriva Franței (5335/06)**
    - Cazul vizează o femeie care a fost concediată de la locul de muncă în urma divulgării, fără consimțământul său, a unei afecțiuni medicale care a fost considerată incompatibilă cu postul său.
    - Reclamanta a susținut că divulgarea informațiilor medicale fără consimțământul său și concedierea în urma acestor informații au încălcat dreptul său la respectarea vieții private și de familie.
    - Soluția CEDO: Curtea a decis că a existat o încălcare a articolului 8 al Convenției și a acordat despăgubiri reclamantei.

Acestea sunt câteva dintre cazurile judecate de CEDO în legătură cu datele medicale, protecția acestora și dreptul la viața privată. Cauzele menționate anterior au abordat diverse aspecte ale problemei, cum ar fi **divulgarea nejustificată a informațiilor medicale personale, accesul la dosarele medicale și protecția intereselor părților implicate**.

Rezultatele acestor cazuri arată că **CEDO** acordă o importanță deosebită **protejării dreptului la viața privată în contextul datelor medicale**, evaluând fiecare situație în funcție de circumstanțele specifice ale cazului și echilibrând interesele și drepturile părților implicate.

5.1 RELEVANȚA NORMELOR RGPD ÎN FUNCȚIE DE ROLURILE OCUPATE DE UN MEDIC

MEDIC - Angajat

Medicul este angajat al unui spital, clinică sau altă instituție medicală și își desfășoară activitatea în cadrul acestei instituții, sub contract de muncă.

Obligații principale specifice R.G.P.D.:

- Să respecte de principiu **orice aspect de viață privată sau de protecția datelor** cu caracter personal întâlnit în desfășurarea activității. În acest sens, operatorul (angajatorul spital sau unitate medicală) poate adopta o serie numeroasă de politici sau proceduri pe care le va aduce la cunoștința angajaților.
- Să respecte normele, chiar și în situația în care **devine operator de date** în calitate de persoană fizică (ex. în situația în care dorește să participe pe cont propriu la un congres științific în care dorește să prezinte informații referitoare la o persoană identificată sau identificabilă).

Cele mai relevante capitole sunt:

- Orientarea 3.6 privind **utilizarea dispozitivelor mobile**
- Orientarea 3.7 cu privire la **utilizarea e-mailului sau a faxului**
- Orientarea 3.8 cu privire la **protejarea datelor în afara cadrului profesional de desfășurare a activității**

- Orientarea 3.13 privitoare la **utilizarea datelor cu caracter personal în scopuri secundare decât cele în care au fost colectate inițial**
- Orientarea 3.15 cu privire la **protejarea datelor atunci când un medic își încetează activitatea**

MEDIC - Administrator al unui cabinet individual

Medicul își desfășoară activitatea într-un cabinet medical propriu, independent de orice instituție sau clinică. Acesta își gestionează propriul cabinet, fiind responsabil pentru toate aspectele administrative, financiare și legale ale afacerii. De obicei, medicul cu cabinet individual își stabilește propriile tarife pentru serviciile medicale oferite și își gestionează programul și relația cu pacienții în mod direct.

Obligații principale specifice R.G.P.D.:

- În calitate de administrator al formei juridice înființate (ex. S.R.L.) poartă **responsabilitatea tuturor operațiunilor de prelucrări de date** desfășurate în cadrul organizației.

Cele mai relevante capitole sunt:

- Toate orientările (3.1 - 3.16) sunt aplicabile în acest sens!
- Cel mai arzător aspect poate fi cel precizat în Orientarea 3.12 privind **modalitatea de răspuns în caz de încălcare a securității și confidențialității datelor pacientului sau a altei persoane vizate**

MEDIC - Colaborator al unui spital / al unei clinici

Medicul colaborează cu un spital sau o clinică în calitate de profesionist independent, fără a fi angajat în mod formal. Acesta își desfășoară activitatea în cadrul instituției, dar nu beneficiază de un salariu fix sau beneficii de angajare. În schimb, medicul colaborator poate primi o remunerație în funcție de serviciile medicale oferite sau poate încheia un contract de colaborare cu instituția, în care sunt stabilite termenii și condițiile colaborării.

Obligații principale specifice R.G.P.D.:

- În calitate de colaborator, se va supune în mod direct politicilor și procedurilor adoptate de unitatea medicală (spital, clinică).

Cele mai relevante capitole sunt:

- Orientarea 3.1 privind a**cordurile de confidențialitate și contractele de servicii încheiate de medici**
- Orientarea 3.8 cu privire la **protejarea datelor în afara cadrului profesional de desfășurare a activității**
- Orientarea 3.9 cu privire la **oferirea de servicii de telemedicină**
- Orientarea 3.12 privind **modalitatea de răspuns în caz de încălcare a securității și confidențialității datelor pacientului sau a altei persoane vizate**
- Orientarea 3.13 privitoare la **utilizarea datelor cu caracter personal în scopuri secundare decât cele în care au fost colectate inițial**

MEDIC - Cadru universitar

Medicul își desfășoară activitatea în cadrul unei universități sau instituții de învățământ superior, predând cursuri și conducând cercetări în domeniul medical. Acesta poate combina activitatea didactică și de cercetare cu practica medicală în cadrul unui spital sau al unei clinici afiliate universității.

Obligații principale specifice R.G.P.D.:

- În calitate angajat al instituției de învățământ superior, va respecta toate politicile și procedurile adoptate intern.
- Se va asigura că nu divulgă datele pacienților săi din spital în activitatea educațională.

Cele mai relevante capitole sunt:

- Orientarea 3.13 privitoare la **utilizarea datelor cu caracter personal în scopuri secundare decât cele în care au fost colectate inițial**
- Orientarea 3.15 cu privire la **protejarea datelor atunci când un medic își încetează activitatea**
- Orientarea 3.16 privind **obținerea și gestionarea consimțământului persoanei vizate**

MEDIC - Consultant

Medicul oferă consultanță și expertiză medicală altor instituții, companii sau organizații într-un domeniu specific al medicinei. Acesta poate fi implicat în dezvoltarea de produse sau servicii medicale, în cercetare și dezvoltare sau în aspecte legate de reglementarea și conformitatea în domeniul sănătății.

Obligații principale specifice R.G.P.D.:

- În calitate consultant, se va asigura că respectă contractul încheiat cu partea terță și obligațiile înscrise în acest contract.

Cele mai relevante capitole sunt:

- Orientarea 3.1 privind **acordurile de confidențialitate și contractele de servicii încheiate de medici**
- Orientarea 3.6 privind **utilizarea dispozitivelor mobile**
- Orientarea 3.7 cu privire la **utilizarea e-mailului sau a faxului**

MEDIC - Cercetător

Medicul se concentrează pe cercetarea științifică într-un domeniu specific al medicinei, contribuind la dezvoltarea de noi tehnici, tratamente și cunoștințe în domeniu. Acesta poate lucra în cadrul unui institut de cercetare, al unei universități sau al unei companii farmaceutice.

Obligații principale specifice R.G.P.D.:

- În calitate de cercetător angajat al unei instituții se va asigura că respectă politicile și procedurile interne specifice protecției datelor.

Cele mai relevante capitole sunt:

- Orientarea 3.13 privitoare la **utilizarea datelor cu caracter personal în scopuri secundare decât cele în care au fost colectate inițial**
- Orientarea 3.16 privind **obținerea și gestionarea consimțământului persoanei vizate**

MEDIC - Voluntar

Medicul oferă servicii medicale în mod voluntar, fără a primi remunerație, în cadrul unor organizații non-profit, misiuni umanitare sau proiecte comunitare. Aceasta poate include participarea la campanii de vaccinare, acordarea de îngrijiri medicale în zone defavorizate sau răspunsul la situații de urgență și dezastre naturale.

Obligații principale specifice R.G.P.D.:

- Medicul voluntar se va asigura că respectă instrucțiunile date de organizația (asociația, instituția) care gestionează activitatea în care este implicat.

Cele mai relevante capitole sunt:

- Orientarea 3.5 cu privire la **posibilitatea de fotografiere, realizarea de capturi video și alte imagini** folosite în serviciul medical
- Orientarea 3.6 privind **utilizarea dispozitivelor mobile**

MEDIC - Autor

Medicul scrie cărți, articole sau materiale educative în domeniul medical, adresate atât profesioniștilor din domeniu, cât și publicului larg. Aceasta poate include scrierea de ghiduri practice, manuale de specialitate sau lucrări științifice publicate în jurnale de specialitate.

Obligații principale specifice R.G.P.D.:

- Să se asigure că pentru materialele incluse în cărți, articole, studii ș.a. folosește strict date statistice sau date anonimizate.
- În cazul în care dorește să folosească și date care pot duce la identificarea persoanei, se va asigura că are consimțământul acesteia.

Cele mai relevante capitole sunt:

- Orientarea 3.13 privitoare la **utilizarea datelor cu caracter personal în scopuri secundare decât cele în care au fost colectate inițial**
- Orientarea 3.16 privind **obținerea și gestionarea consimțământului persoanei vizate**

MEDIC - Antreprenor

Medicul își deschide și conduce propria afacere în domeniul sănătății, care poate include o clinică, un laborator de analize medicale, o companie farmaceutică sau de dispozitive medicale, sau orice altă afacere legată de domeniul medical.

Obligații principale specifice R.G.P.D.:

- La fel ca și în cazul medicului administrator a unei persoane juridice, pentru fiecare structură înființată trebuie să respecte normele de protecție a datelor.
- Se va asigura că transferurile de date sunt realizate în conformitate cu R.G.P.D. (ex. dacă se transferă datele de la o clinică proprie la un laborator de analize propriu)

Cele mai relevante capitole sunt:

- Toate orientările (3.1 - 3.16) sunt aplicabile în acest sens!

MEDIC - Formator

Medicul oferă instruire și educație medicală colegilor, rezidenților și studenților în cadrul unor instituții de învățământ superior, spitale sau clinici. Acesta poate fi implicat în programe de pregătire postuniversitară sau în dezvoltarea de cursuri și materiale didactice.

Obligații principale specifice R.G.P.D.:

- Să se asigure că pentru materialele incluse în cărți, articole, studii ș.a. folosește strict date statistice sau date anonimizate.
- În cazul în care dorește să folosească și date care pot duce la identificarea persoanei, se va asigura că are consimțământul acesteia.

Cele mai relevante capitole sunt:

- Orientarea 3.13 privitoare la **utilizarea datelor cu caracter personal în scopuri secundare decât cele în care au fost colectate inițial**
- Orientarea 3.16 privind **obținerea și gestionarea consimțământului persoanei vizate**

MEDIC - Legist

Medicul legist se specializează în medicina legală și investigația cauzelor de deces, ajutând la soluționarea cazurilor juridice și la elucidarea circumstanțelor decesului. Acesta poate lucra în cadrul unor instituții guvernamentale, laboratoare de medicină legală sau ca expert în cazurile judiciare.

Obligații principale specifice R.G.P.D.:

- Va respecta procedurile și politicile instituției în care își desfășoară activitatea.
- Atenție! Deși normele R.G.P.D. caută să protejeze datele de identificare ale persoanelor fizice în viață, prelucrarea neconformă a datelor persoanei decedate poate, în anumite cazuri, atrage nemulțumirea rudelor acestuia.

Cele mai relevante capitole sunt:

- Orientarea 3.11 cu privire la **gestionarea reclamațiilor angajaților respectiv pacienților**

MEDIC - Expert medical în asigurări

Medicul lucrează în cadrul companiilor de asigurări, evaluând cererile de despăgubire, analizând dosarele medicale și oferind sfaturi în probleme legate de sănătate. Acesta poate fi implicat și în dezvoltarea de produse de asigurare în domeniul sănătății.

Obligații principale specifice R.G.P.D.:

- Va respecta procedurile și politicile companiei în care activează.
- Dacă este implicat în dezvoltarea de produse de asigurare în domeniul sănătății, se va asigura că nu va expune datele de identificare ale pacienților cu care a interacționat în activitatea medicală.

Cele mai relevante capitole sunt:

- Orientarea 3.13 privitoare la **utilizarea datelor cu caracter personal în scopuri secundare decât cele în care au fost colectate inițial**
- Orientarea 3.16 privind **obținerea și gestionarea consimțământului persoanei vizate**

MEDIC - Telemedicină

Medicul furnizează îngrijiri medicale și consultații la distanță, utilizând tehnologii de comunicație și informație pentru a evalua, diagnostica și trata pacienți în zone îndepărtate sau cu acces limitat la servicii medicale.

Obligații principale specifice R.G.P.D.:

- Se va asigura că platformele și aplicațiile folosite sunt în conformitate cu normele R.G.P.D. prin verificarea termenilor și condițiilor aplicației, a politicii de confidențialitate sau a altor angajamente specifice luate de dezvoltator.

Cele mai relevante capitole sunt:

- Orientarea 3.3 privind **regulile de acces la bazele de date electronice**
- Orientarea 3.9 cu privire la **oferirea de servicii de telemedicină**

MEDIC - Activist pentru drepturile pacienților

Medicul militează pentru protejarea și promovarea drepturilor pacienților, având ca scop îmbunătățirea calității și accesibilității serviciilor medicale, precum și conștientizarea problemelor de sănătate și necesitatea unui sistem de sănătate echitabil și eficient.

Obligații principale specifice R.G.P.D.:

- Se va asigura că nu realizează divulgări de date cu caracter personal ale pacienților în spațiul public (ex. prin meetinguri, interviuri televizate, postări pe rețele de socializare) în lipsa consimțământului acestuia.

Cele mai relevante capitole sunt:

- Orientarea 3.13 privitoare la **utilizarea datelor cu caracter personal în scopuri secundare decât cele în care au fost colectate inițial**
- Orientarea 3.16 privind **obținerea și gestionarea consimțământului persoanei vizate**

MEDIC - Expert în politici de sănătate

Medicul lucrează în cadrul guvernamental sau al organizațiilor internaționale, contribuind la elaborarea, implementarea și evaluarea politicilor de sănătate publică. Acesta poate fi implicat în elaborarea de strategii și programe pentru combaterea bolilor, promovarea sănătății și prevenirea îmbolnăvirilor, sau monitorizarea și evaluarea sistemelor de sănătate.

Obligații principale specifice R.G.P.D.:

- Se va asigura că respectă politicile și procedurile organizației în care își desfășoară activitatea.
- Nu se va folosi de date cu caracter personal colectate în cadrul activității medicale desfășurate, în lipsa consimțământului persoanei vizate (ex. pacient).

Cele mai relevante capitole sunt:

- PARTEA I - Introducere în Protecția Datelor în sistemul medical românesc
  - Cadrul legislativ și aplicabilitatea R.G.P.D.
  - Locul dreptului la protecția datelor medicale în sistemul juridic
  - Principiile protecției datelor
  - Temeiurile legitime și situații speciale ale prelucrărilor de date
- Orientarea 3.13 privitoare la **utilizarea datelor cu caracter personal în scopuri secundare** decât cele în care au fost colectate inițial
- Orientarea 3.16 privind **obținerea și gestionarea consimțământului persoanei vizate**

MEDIC - Coordonator de programe medicale

Medicul coordonează și supervizează programe medicale și proiecte speciale, asigurându-se de implementarea corectă a acestora și atingerea obiectivelor propuse. Acesta poate lucra în cadrul unui spital, al unei clinici, al unei organizații non-profit sau al unei companii din domeniul sănătății.

Obligații principale specifice R.G.P.D.:

- Se asigură că sunt respectate toate normele specifice R.G.P.D. în programul medical dezvoltat.
- Colaborează cu Responsabilul cu Protecția Datelor al organizației.

Cele mai relevante capitole sunt:

- Orientarea 3.3 privind **regulile de acces la bazele de date electronice**

MEDIC - Specialist în informatică medicală

Medicul combină cunoștințele medicale cu expertiza în tehnologie și informatică pentru a dezvolta, implementa și îmbunătăți sistemele informatice utilizate în domeniul sănătății. Aceasta poate include lucrul cu sistemul electronic de sănătate, analiza de date medicale sau dezvoltarea de aplicații și instrumente digitale pentru îmbunătățirea îngrijirii pacienților.

Obligații principale specifice R.G.P.D.:

- Se asigură că sunt respectate toate normele specifice R.G.P.D. în programul medical dezvoltat.
- Nu se va folosi de date cu caracter personal colectate în cadrul activității medicale desfășurate, în lipsa consimțământului persoanei vizate
- Colaborează cu Responsabilul cu Protecția Datelor al organizației pentru înțelegerea cerințelor art. 25 din R.G.P.D. și modalitatea în care acestea sunt implementate și respectate.

Cele mai relevante capitole sunt:

- Orientarea 3.3 privind **regulile de acces la bazele de date electronice**
- Orientarea 3.14 privind **distrugerea în siguranță a datelor cu caracter personal**

MEDIC - Specialist în managementul calității

Medicul se ocupă de implementarea și menținerea standardelor de calitate în domeniul sănătății, evaluând și monitorizând performanțele spitalelor, clinicilor și personalului medical. Acesta poate contribui la elaborarea de politici și proceduri pentru îmbunătățirea calității îngrijirilor medicale.

Obligații principale specifice R.G.P.D.:

- Se asigură că ia la cunoștință despre normele R.G.P.D. și colaborează cu Responsabilul cu Protecția Datelor al organizației pentru a implementa politicile și procedurile necesare inclusiv pentru respectarea vieții private și a datelor cu caracter personal.

Cele mai relevante capitole sunt:

- PARTEA I - Introducere în Protecția Datelor în sistemul medical românesc.
  - Principiile protecției datelor, Temeiurile legitime și situații speciale ale prelucrărilor de date, Drepturile persoanelor vizate
- Toate orientările specifice (3.1 - 3.16)

MEDIC - Specialist în sănătate ocupațională

Medicul se ocupă de prevenirea și managementul problemelor de sănătate legate de mediul de muncă, evaluând riscurile pentru sănătate și oferind sfaturi în probleme de ergonomie, securitate la locul de muncă și promovarea sănătății angajaților.

Obligații principale specifice R.G.P.D.:

- Respectă politicile și procedurile organizației la care lucrează sau cu care colaborează

Cele mai relevante capitole sunt:

- Orientarea 3.1 privind **acordurile de confidențialitate și contractele de servicii încheiate de medici**
- Orientarea 3.2 privind **angajamentele de confidențialitate luate în relațiile de muncă**
- Orientarea 3.12 privind **modalitatea de răspuns în caz de încălcare a securității și confidențialității datelor pacientului sau a altei persoane vizate**

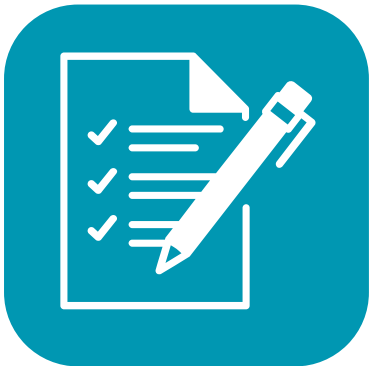
5.2 DEFINIȚII GRAFICE

OPERATOR DE DATE

Persoana fizică sau juridică care, singur sau împreună cu altele, stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal. **Exemplu**: spital, clinică, altă formă de exercitare a profesiei

PERSOANA VIZATĂ

Persoana fizică ale cărei date sunt prelucrate (colectate, înregistrate, comunicate etc.) **Exemplu**: pacient, aparținător sau chiar angajatul unui operator de date.



DATE CU CARACTER PERSONAL

Orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată”). **Exemplu**: nume, prenume, CNP, date referitoare la starea de sănătate ș.a.

PERSOANA ÎMPUTERNICITĂ

Persoana fizică sau juridică ce prelucrează date cu caracter personal în numele operatorului. **Exemplu**: furnizor de servicii de curierat, furnizor de servicii de securitate informatică, etc.

PRELUCRARE DE DATE

Orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal. **Exemplu:** colectare, stocare, ștergere, transmitere, divulgare / punere la dispoziție, etc.

TEMEI LEGAL

Baza juridică ce justifică prelucrarea datelor cu caracter personal ăn conformitate cu legislația. **Exemplu**: obligație legală, executare contract, consimțământ, inters vital, etc.

INCIDENT / BREȘĂ DE SECURITATE

O încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea sau divulgarea neautorizată a datelor cu caracter personal. **Exemplu**: s-a pierdut o foaie de observație, o persoană a primit în mod neautorizat datele medicale ale altei persoane, etc.

CALITATEA MEDICULUI - ANGAJAT

MEDICUL ESTE PERSOANĂ VIZATĂ CÂND:

Este angajat în cadrul unei unități medicale și propriile date sunt prelucrate. Exemplu: în cadrul proceselor de salarizare îi sunt prelucrate date precum contul bancar, etc.

Este medicul angajat o persoană împuternicită a operatorului (spital / clinică)?

Angajații operatorului de date NU sunt considerați persoane împuternicite. Atâta timp cât o persoană acționează în cadrul atribuțiilor sale de serviciu, aceasta acționează ca un reprezentant (agent) al operatorului de date.

Cu alte cuvinte, RGPD îi va considera ca făcând parte din entitatea operatorului de date şi nu ca o parte separată care este angajată să prelucreze date în numele operatorului de date.

Exemplu: Consulturile medicale pe care un medic le face, tratamentele pe care le administrează sau alte asemenea, fac parte din sarcinile medicului care acționează în calitate de parte a spitalului în oferirea de servicii medicale.

Drepturile medicului în calitatea sa de angajat:

- beneficiază de toate drepturile unei persoane vizate în relație cu angajatorul

Responsabilitățile medicului (semnează CIM):

- îndeplinirea obligațiilor conform CCM, CIM, fișa postului, etc.
- respectarea politicilor și procedurilor interne care impun obligații specifice protecției datelor

Răspunderea medicului:

- ca regulă generală, răspunde strict în baza dreptului muncii pentru nerespectarea obligațiilor de mai sus
- răspunde când își depășește sfera atribuțiilor de serviciu și devine **operator de date**
- operatorul (spital / clinică) poartă răspunderea principală pentru încălcările protecției datelor, cel mai adesea

CALITATEA MEDICULUI ADMINISTRATOR AL PERSOANEI JURIDICE (SRL, PFI, PFA)

MEDICUL ESTE OPERATOR DE DATE CÂND:

- Înființează o persoană juridică / devine administratorul unei persoane juridice care oferă servicii medicale și prelucrează orice fel de date ale angajaților, pacienților, colaboratorilor, etc.

- Își depășește sfera atribuțiilor de serviciu (în calitate de angajat) și prelucrează date în scopuri și cu mijloace proprii. **Exemplu**: fotografiază analizele medicale și le postează pe blogul propriu ca informații referitoare la "studiul de caz" dat.

Drepturile medicului în calitatea sa de administrator:

- limitate (puține) întrucât RGPD protejează persoanele fizice și datele acestora de identificare, nu ale persoanelor juridice

Responsabilitățile medicului (semnează contracte cu furnizori de servicii):

- să implementeze politici, proceduri specifice protecției datelor (ex. plan de reacție la incidente)
- să ia măsuri tehnice și organizatorice specifice protecției datelor (ex. instruirea personalului)

Răspunderea medicului:

- răspunde în baza legii (RGPD)

MEDICUL ESTE OPERATOR ASOCIAT CÂND:

- Colaborează cu un operator de date (ex. clinică) dar are un nivel de control asupra scopului și mijloacelor de prelucrare a datelor. **Exemplu**: o clinică medicală colaborează cu un medic radiolog care își desfășoară activitatea prin intermediul propriului SRL/PFI/PFA și are propriul său echipament de diagnosticare prin imagistică.

Drepturile medicului în calitatea sa de operator asociat:

- limitate (puține) întrucât RGPD protejează persoanele fizice și datele acestora de identificare, nu ale persoanelor juridice

Responsabilitățile medicului:

- să implementeze propriile politici, proceduri specifice prin care să protejeze datele care ajung în sfera proprie de activitate

Răspunderea medicului:

- răspunde în baza legii (RGPD)
- răspunde conform contractului dintre părți

MEDICUL ESTE PERSOANĂ ÎMPUTERNICITĂ CÂND:

- Medicul se folosește de bazele de date, infrastructura sau mijloacele puse la dispoziție de unitatea medicală și acționează în numele ei, urmând instrucțiunile acesteia. **Exemplu**: o clinică medicală contractează serviciile unui medic specialist pentru a oferi evaluări și tratamente specifice pacienților săi.

Drepturile medicului în calitatea sa de persoană împuternicită:

- limitate (puține) întrucât RGPD protejează persoanele fizice și datele acestora de identificare, nu ale persoanelor juridice

Responsabilitățile medicului (semnează contracte de servicii):

- să implementeze propriile politici, proceduri specifice prin care să ofere un nivel asemănător de protecție a datelor precum cel al operatorului

Răspunderea medicului:

- răspunde în baza legii (RGPD)
- răspunde conform contractului dintre părți

MEDIC - ANGAJAT

PERSOANĂ VIZATĂ

- semnează Contract individual de muncă
- respectă politici și proceduri interne ale angajatorului
- răspunde conform CIM

OPERATOR DE DATE

- acționează dincolo de atribuțiile de serviciu
- răspunde în baza legii (RGPD)

MEDIC - ADMINISTRATOR

OPERATOR DE DATE

- semnează contracte cu furnizori de servicii
- implementează politici și proceduri interne
- instruiește personalul pv protecția datelor
- răspunde conform legii (RGPD)

OPERATOR ASOCIAT

- semnează contract de servicii medicale cu altă clinică
- utilizează aparatura medicală proprie
- stabilește propriile politici și proceduri
- răspunde conform legii și conform contract de servicii

PERSOANĂ ÎMPUTERNICITĂ

- semnează contract de servicii medicale cu altă clinică
- utilizează aparatura medicală a clinicii
- respectă politicile și procedurile interne
- răspunde conform legii și conform contract de servicii

ANEXA 1

Model de clauze care ar trebui preluate în relație cu angajații

REGULAMENTUL INTERN se va completa cu următoarele:

Dispoziții generale - Reguli privind confidențialitatea, securitatea și protecția datelor cu caracter personal.

Baza legală:
Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date, și de abrogare a Directivei nr. 95/46/CE („Regulamentul general privind protecția datelor", denumit în continuare „RGPD"), cu Legea nr. 190 din 18.07.2018 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, variantele actualizate la zi și cu celelalte dispoziții legale relevante în materia protecției datelor cu caracter personal.

CAP._____ PROTECȚIA DATELOR CU CARACTER PERSONAL
Art.___ [Operatorul] garantează confidențialitatea datelor cu caracter personal ale salariaților, în conformitate cu dispozițiile RGPD, a Legii nr. 190 din 18.07.2018 care reglementează măsurile necesare punerii în aplicare la nivel național a RGPD, a deciziilor Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum și a celorlalte dispoziții legale relevante în materia protecției datelor cu caracter personal.

Art.___ Conform art. 4 pct. 2 din RGPD, prelucrarea datelor cu caracter personal se referă, fără a se limita la, orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea.

Art.___ [Operatorul], în calitate de Operator de date, respectă și aplică **principiile de prelucrarea a datelor cu caracter personal** prevăzute de RGPD, după cum urmează:

- principiul legalității, echității și transparenței prevăzut la art. 5 alin. (1) lit. a) din RGPD
- principiul limitării legate de scop prevăzut la art. 5 alin. (1) lit. b) din RGPD – conform căruia datele cu caracter personal trebuie să fie colectate în scopuri determinate, explicite și legitime, nefiind permisă prelucrarea ulterioară într-un mod incompatibil acestor scopuri;
- principiul reducerii la minimum a datelor prevăzut la art. 5 alin. (1) lit. c) din RGPD – conform căruia datele cu caracter personal prelucrate trebuie să fie adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate;
- principiul exactității prevăzut la art. 5 alin. (1) lit. d) din RGPD – conform căruia datele cu caracter personal prelucrate trebuie să fie exacte și, în cazul în care este necesar, trebuie să fie actualizate; în acest sens, datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, trebuie să fie șterse sau rectificate fără întârziere;
- principiul limitării legate de scop prevăzut la art. 5 alin. (1) lit. e) din RGPD – conform căruia datele cu caracter personal trebuie să fie păstrate într-o formă care să permită identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate;
- principiul securității și confidențialității prevăzut la art. 5 alin. (1) lit. f) din RGPD – conform căruia datele cu caracter personal trebuie să fie prelucrate într-un mod care asigură securitatea adecvată a datelor, inclusiv protecția împotriva prelucrării neautorizate sau ilegale, împotriva pierderii, a distrugerii sau a deteriorării accidentale;
- principiul responsabilității prevăzut la art. 24 alin. (1) din RGPD – conform căruia trebuie să fie luate măsuri tehnice și organizatorice adecvate pentru a garanta și demonstra că prelucrarea se efectuează în conformitate cu RGPD, măsuri care vor fi revizuite și actualizate în mod activ;
- principiul protecției datelor cu caracter personal începând cu momentul conceperii prevăzut la art. 25 alin. (2) din RGPD.

Art.___ [Operatorul], în calitate de Operator de date, are următoarele **drepturi și obligații generale**:

- dreptul de a da dispoziții cu caracter obligatoriu pentru salariat în ceea ce privește modalitatea de prelucrare a datelor cu caracter personal, conform RGPD și a legislației naționale relevante în materia protecției datelor cu caracter personal;
- dreptul de a realiza prelucrări de date cu caracter personal, potrivit competențelor atribuite de lege și de alte acte normative de punere în aplicare și de a constitui și utiliza baza de date potrivit legii;
- dreptul de a prelucra date cu caracter personal în vederea încheierii și executării contractelor de muncă și a celorlalte raporturi de muncă specific statutului de funcționar public;
- obligația de a prelucra datele cu caracter personal ale salariatului în strictă conformitate cu prevederile RGPD și a legislației naționale relevante în materia protecției datelor cu caracter personal.

Art.___Reguli generale privind gestionarea și prelucrarea datelor cu caracter personal:

- Datele cu caracter personal se stochează numai pentru perioada necesară atingerii scopurilor stabilite, perioadele minime și maxime pentru stocarea datelor colectate fiind prevăzute în politicile interne ale **[Operatorul]**, având în vedere obligația de respectare a drepturilor persoanei vizate, în special a dreptului de acces, de intervenție și de a fi uitat.
- În urma verificărilor periodice, datele cu caracter personal deținute de **[Operatorul]**, care nu mai servesc realizării scopurilor sau îndeplinirii unor obligații legale, vor fi distruse, șterse sau anonimizate.

Art.___ Salariatul, în calitate de persoană vizată, are următoarele **drepturi generale:**

- dreptul la protecția datelor cu caracter personal
- dreptul la informare, acces, rectificare, ștergere, opoziție, portabilitate, restricționarea prelucrării datelor cu caracter personal și de a nu fi subiectul unei decizii bazate exclusiv pe prelucrare automatizată, în condițiile și limitele RGPD și a legislației naționale relevante în materia protecției datelor cu caracter personal.

Art.___ (1) Cererea de exercitare a drepturilor prevăzute de RGPD, va fi adresată Responsabilului cu protecția datelor. **(2)** Cererea se soluționează în termen de 30 de zile de la data comunicării acesteia, pe parcursul căruia salariatul poate să furnizeze Responsabilului cu protecția datelor informațiile utile soluționării cererii. **(3)** Politica de exercitare a drepturilor prevăzute de RGPD constituie anexă la Regulamentul de Ordine Interioară.

Art.___Salariatul are următoarele **obligații**:

- de a prelucra datele cu caracter personal numai pentru aducerea la îndeplinire a atribuțiilor de serviciu prevăzute în Fișa postului, în Contractul individual de muncă și în Regulamentul de Ordine Interioară, și în conformitate cu și în limitele de autorizare stabilite în procedurile interne ale [Operatorul]. Datele cu caracter personal nu pot fi prelucrate ulterior în alte scopuri incompatibile cu scopul în care acestea au fost inițial colectate;
- de a nu întreprinde nimic de natură să aducă atingere protecției necesare a datelor cu caracter personal prelucrate sau de care iau cunoștință cu ocazia îndeplinirii atribuțiilor de serviciu;
- de a păstra confidențialitatea asupra datelor cu caracter personal pe care le prelucrează, respectiv de a nu dezvălui datele cu caracter personal pe care le prelucrează unor alte persoane decât cele în privința cărora le este permis acest lucru conform procedurilor interne, Regulamentului de Ordine Interioară, a Contractului individual de muncă și a Fișei postului;
- de a respecta măsurile tehnice și organizatorice stabilite pentru protejarea datelor cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat, în special dacă prelucrarea respectivă comportă transmisii de date în cadrul unei rețele, precum și împotriva oricărei alte forme de prelucrare ilegală;
- de a depune toate diligențele necesare pentru prevenirea incidentelor de securitate și de a participa la diminuarea pagubelor în măsura în care un astfel de incident de securitate s-a produs;
- de a aduce la cunoștința [Operatorul] în cel mai scurt timp posibil orice suspiciune de acces neautorizat la datele personale pe care le prelucrează;

- de a informa imediat și detaliat, în scris, superiorul ierarhic sau Responsabilul cu protecţia datelor cu caracter personal în legătură cu orice nelămurire, suspiciune sau observație cu privire la protecția datelor cu caracter personal ale salariaților, ale clienților, ale colaboratorilor **[Operatorul]**, în legătură cu orice divulgare a datelor cu caracter personal și în legătură cu orice incident de natură să ducă la divulgarea datelor cu caracter personal de care iau cunoștință, în virtutea atribuțiilor de serviciu și în orice altă împrejurare, prin orice mijloace. Dacă pericolul cu privire la datele cu caracter personal este iminent, informarea se va face telefonic și în scris. Încălcarea obligației de informare constituie abatere disciplinară.

Art.___Respectarea politicilor și procedurilor privind protecția datelor:

- Salariații se obligă să respecte cu strictețe politicile și procedurile privind protecția datelor ale **[Operatorul]**, care vor fi aduse la cunoștința acestora prin grija conducerii și/sau persoanelor delegate în acest sens.
- Salariații vor realiza, revizui și actualiza periodic Registrul de activități de prelucrare a datelor cu caracter personal.
- Salariații sunt obligați să participe la toate training-urile, instruirile și ședințele de informare organizate de **[Operatorul]** cu privire la protecția datelor cu caracter personal.

Art.___ Pe toată perioada derulării contractului individual de muncă, precum și după încetarea acestuia, pe o perioadă nelimitată, indiferent de motivele acestei încetări, salariații vor respecta caracterul confidențial al datelor cu caracter personal pe care le-au cunoscut în orice mod, ca urmare a încheierii și executării contractului individual de muncă, și caracterul confidențial al informațiilor privitoare la prelucrarea datelor cu caracter personal.

Art.___ Răspundere:
Nerespectarea obligațiilor prevăzute în prezentul capitol și a oricăror reguli, politici, proceduri și instrucțiuni interne cu privire la protecția datelor cu caracter personal atrage răspunderea disciplinară și/sau patrimonială a salariaților, constituind abatere disciplinară și se sancționează în conformitate cu prevederile Regulamentului de Ordine Interioară și a legislației relevante aplicabile.

CONTRACTUL INDIVIDUAL DE MUNCĂ se va completa cu următoarele:

Drepturile salariatului se completează cu:

- Dreptul la protecția datelor cu caracter personal;
- Dreptul la informare, acces, rectificare, ștergere, opoziție, portabilitate, restricționarea prelucrării datelor cu caracter personal și de a nu fi subiectul unei decizii bazate exclusiv pe prelucrare automatizată, în condițiile și limitele Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (,,Regulamentul general privind protecția datelor'') și a legislației naționale relevante în materia protecției datelor cu caracter personal.

Obligațiile salariatului se completează cu:

- Obligația de a respecta reglementările, politicile și procedurile interne adoptate la nivelul Angajatorului și indicațiile acestuia date în vederea conformării cu Regulamentul general privind protecția datelor și legislația națională relevantă aplicabilă în materia protecției datelor cu caracter personal.

Drepturile angajatorului se completează cu:

- Dreptul de a da dispoziții cu caracter obligatoriu pentru salariat, inclusiv în ceea ce privește modalitatea de prelucrare a datelor cu caracter personal conform standardelor Regulamentului general privind protecția datelor și a legislației naționale relevante aplicabile în materia protecției datelor cu caracter personal.

Obligațiile angajatorului se completează cu:

- Obligația să prelucreze datele cu caracter personal ale salariatului în strictă conformitate cu prevederile Regulamentului general privind protecția datelor și a legislației naționale relevante în materia protecției datelor cu caracter personal.

FIȘA POSTULUI se va completa cu următoarele:

Aplicabil pentru oricare dintre funcțiile ocupate:

- Să prelucreze datele cu caracter personal în strictă conformitate cu prevederile Regulamentului General privind Protecția Datelor și a legislației naționale în domeniu, și să asigure respectarea și confidențialitatea acestor date cu caracter personal;
- Să instituie politici și proceduri interne privind protecția datelor cu caracter personal conform prevederilor legale aplicabile; (aplicabil doar persoanei cu funcție de conducere)
- Să instituie măsuri tehnice și organizatorice în vederea asigurării protecției datelor cu caracter personal;
- Să păstreze confidențialitatea datelor cu caracter personal prelucrate, a contului de utilizator, a parolei/codului de acces la sistemele informatice/ baze de date prin care sunt gestionate date cu caracter personal;
- Să informeze de îndată Responsabilul cu protecția datelor despre împrejurări de natură a conduce la o divulgare neautorizată de date cu caracter personal sau despre o situație în care au fost accesate/ prelucrate date cu caracter personal prin încălcarea normelor legale, despre care a luat cunoștință;
- Să coopereze cu Responsabilul cu protecția datelor în soluționarea cererilor de exercitare a drepturilor conferite de Regulamentul general privind protecția datelor;
- Să solicite în scris consiliere din partea Responsabilului cu protecția datelor în cazul în care identifică riscuri cu privire la prelucrarea datelor cu caracter personal.

ANEXA 2

Model de Acord de confidențialitate pe care să îl utilizați în relație cu colaboratorii persoane împuternicite

ANEXA _____
la Contractul nr._____ din _____

1) Prevederi generale:

- Părțile prelucrează date cu caracter personal în **scopul**:
  - încheierii și executării Contractului, conform art. 6 alin. (1) lit. b) din RGPD;
  - îndeplinirii obligațiilor legale ce le revin, conform art. 6 alin. (1) lit. c) din RGPD;
  - îndeplinirii îndeplinirea unei sarcini care servește unui interes public conform art. 6 alin. (1) lit. e) din RGPD;
- Prelucrarea datelor cu caracter personal se face **prin mijloacele și conform cerințelor** prevăzute în legislația specială aplicabilă fiecărei Părți (operator sau persoană împuternicită), conform obiectului de activitate al acesteia, respectând garanțiile impuse de RGPD.
- În executarea contractului, Părțile prelucrează următoarele **categorii de date**: *Nume, prenume, funcție, serie și număr C.I., CNP (după caz), date referitoare la starea de sănătate, semnătură, email sau alte date de contact.*
- Persoanele vizate sunt: reprezentanți legali ai diferitelor societăți; persoanele de contact, alte persoane vizate precum pacienți, aparținători ș.a.
- Datele cu caracter personal sunt stocate în vederea prelucrării lor pe **durata necesară** atingerii scopurilor de prelucrare menționate în contract, sau pe durata impusă de lege, în vederea îndeplinirii unor obligații legale care incumbă Părților (ex. arhivare).
- **Părțile, având calitatea de operator** (**Denumirea societății - ex. SC Clinica SRL**) și **Persoană Împuternicită (Denumirea societății - ex. SC. Doctor SRL; SC Curier SRL; SC Firma IT SRL)**, conform RGPD, se obligă să ia toate măsurile prevăzute de regulament astfel încât să poată conformitatea cu **principiile de prelucrare a datelor cu caracter personal** conform art. 5; dar și cu toate prevederile specifice (ex. art. 28, art. 32).

- **Datele de contact** ale Responsabilului cu Protecția Datelor / Persoanei cu atribuții în domeniul protecției datelor sunt:
    - Pentru Operator: *(se indică emailul)*
    - Pentru Persoana Împuternicită: *(se indică emailul)*

2) Obligații specifice persoanei împuternicite:

- Persoană împuternicită de operator, prelucrează datele cu caracter personal **numai pe baza unor instrucțiuni documentate din partea operatorului**, cu excepția cazului în care această obligație îi revine persoanei împuternicite în temeiul dreptului Uniunii sau al dreptului intern care i se aplică; în acest caz, notifică această obligație juridică operatorului înainte de prelucrare, cu excepția cazului în care dreptul respectiv interzice o astfel de notificare din motive importante legate de interesul public;
- Persoana Împuternicită garantează **asumarea obligației de confidențialitate și securitate a datelor** prin dispunerea de măsuri tehnice și organizatorice, conform prevederilor art. 32, astfel încât să fie stabilite persoanele autorizate să prelucreze datele cu caracter personal, să fie stabilit fluxul și circuitul datelor cu caracter personal exclusiv potrivit prevederilor legale și clauzelor contractuale dintre părți, precum și să existe măsuri de asigurare a securității și integrității datelor cu caracter personal prelucrate în executarea și derularea Contractului. Această obligație va fi transmisă oricărui membru a persoanei împuternicite sau oricărei părți contractate cu acordul Operatorului.
- În cazul în care **datele cu caracter personal au fost accesate sau obținute de o persoană neautorizata** sau are loc **orice încălcare a securității datelor cu caracter personal**, Persoana Împuternicită va notifica de îndată Operatorul un astfel de incident în maximum 24 ore de la luarea la cunoștință, și se va asigura că va lua orice măsuri considerate necesare pentru atenuarea oricărei pierderi sau daune provocate de un astfel de acces neautorizat. În cadrul notificării trimise către Operator, Persoana Împuternicită va furniza cel puțin următoarele informații:
    - o descriere a naturii încălcării protecției datelor cu caracter personal, inclusiv, dacă este posibil, numărul aproximativ al persoanelor vizate în cauză;
    - o descriere a consecințelor probabile ale încălcării securității datelor cu caracter personal;
    - o descriere a măsurilor adoptate sau propuse pentru remedierea încălcării securității datelor cu caracter personal și, dacă este necesar, a măsurilor pentru atenuarea efectelor negative ale acestora.

- Persoana Împuternicită se va asigura că accesul la datele cu caracter personal este strict limitat la angajații, colaboratorii sau alte persoane autorizate ale persoanei împuternicită care au nevoie să cunoască sau să acceseze datele cu caracter personal relevante, după cum este strict necesar în scopul Contractului.
- Persoana Împuternicită se va asigura că toate persoanele autorizate să prelucreze datele cu caracter personal ale persoanelor vizate au încheiat acorduri de confidențialitate sau sunt ținute de o obligație legală de confidențialitate.
- Persoana Împuternicită, la alegerea operatorului, șterge sau returnează operatorului toate datele cu caracter personal după încetarea furnizării serviciilor legate de prelucrare și elimină copiile existente, cu excepția cazului în care dreptul Uniunii sau dreptul intern impune stocarea datelor cu caracter personal;
- Persoana Împuternicită pune la dispoziția operatorului toate informațiile necesare pentru a demonstra respectarea obligațiilor prevăzute de RGPD, permite desfășurarea auditurilor, inclusiv a inspecțiilor, efectuate de operator sau alt auditor mandatat și contribuie la acestea.
- În cazul în care o persoană împuternicită de un operator recrutează o altă persoană împuternicită pentru efectuarea de activități de prelucrare specifice în numele operatorului, aceleași obligații privind protecția datelor prevăzute în contract revin celei de a doua persoane împuternicite, în special furnizarea de garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea să îndeplinească cerințele RGPD. În cazul în care această a doua persoană împuternicită nu își respectă obligațiile privind protecția datelor, persoana împuternicită inițială rămâne pe deplin răspunzătoare față de operator în ceea ce privește îndeplinirea obligațiilor acestei a doua persoane împuternicite.

3**) Obligații privind respectarea drepturilor persoanei vizate:**

- Părțile se asigură că **informarea persoanei vizate este realizată de către fiecare dintre părți**. Informarea se realizează conform procedurilor și politicilor interne adoptate de aceasta.
- Părțile vor asigura **respectarea drepturilor persoanelor vizate**, cu privire la prelucrarea datelor cu caracter personal. Persoana vizată poate să își exercite drepturile legale în mod direct față de oricare dintre Părți, Partea sesizată încunoștințând cealaltă Parte imediat cu privire la orice solicitare primită.

- Părțile se vor sprijini în realizarea obligațiilor contractuale dintre cei doi, atunci când aceasta este necesară pentru soluționarea cererilor de exercitare a drepturilor persoanelor vizate, respectarea obligațiilor privind securitatea datelor cu caracter personal, a obligațiilor de notificare în caz de încălcare a securității datelor, realizarea evaluărilor de impact al protecției datelor și consultărilor prealabile.
- **Fiecare Parte o va notifica pe cealaltă fără întârziere**, în maximum 24 de ore de la primirea solicitării, în cazul în care o autoritate de supraveghere o contactează în mod direct cu privire la activitățile de prelucrare care fac obiectul Contractului.

ANEXA 3

Date identificare operator
Tabel centralizator monitorizare erori

DATE IDENTIFICARE OPERATOR

Acest document se va completa ulterior obținerii consimțămintelor pentru urmărirea cu ușurință a exercitării drepturilor.

DENUMIRE OPERATOR	
DATE DE IDENTIFICARE	
PERSOANA CU ATRIBUȚII ÎN DOMENIUL PROTECȚIEI DATELOR	
DATE DE CONTACT	**EMAIL**
	TELEFON

TABEL CENTRALIZATOR MONITORIZARE ERORI

NR. CRT.	DATA DESCOPERIRII	TIPUL ERORII	DESCRIEREA ERORII	PERSONAL IMPLICAT	CAUZELE POTENȚIALE	ACȚIUNI DE ÎMBUNĂTĂȚIRE	DATA IMPLEMENTĂRII ACȚIUNILOR	RESPONSABIL ACȚIUNI	REZULTAT
1	01.01.2023	Eroare de date personale	Nume incorect	Registrator	Introducere manuală	Verificare dublă	15.01.2023	Manager	Rezolvat

Explicații:

Nr. Crt. - Numărul curent al erorii raportate
Data descoperirii - Data când a fost descoperită eroarea
Tipul erorii - Categoria erorii (ex: eroare de date personale, eroare de diagnostic, eroare în prescripția tratamentului, etc.)
Descrierea erorii - O scurtă descriere a erorii
Personal implicat - Persoana sau persoanele implicate în eroarea respectivă
Cauzele potențiale - Motivele posibile pentru care s-a produs eroarea
Acțiuni de îmbunătățire - Măsuri propuse pentru a preveni reapariția erorii
Data implementării acțiunilor - Data când au fost implementate acțiunile de îmbunătățire
Responsabil acțiuni - Persoana responsabilă de implementarea acțiunilor de îmbunătățire
Rezultat - Starea finală a erorii (ex: rezolvat, în curs de rezolvare, nerezolvat)

!NB - Acest tabel poate fi actualizat în mod constant, astfel încât să reflecte toate erorile întâlnite pe parcursul anului și să permită analiza acestora pentru a identifica posibilele probleme și a îmbunătăți procesele de gestionare a informațiilor.

Este important să comunicați cu personalul implicat și să discutați despre cele mai bune practici, astfel încât să se poată preveni erorile în viitor.

ANEXA 4

Consimțământ specific R.G.P.D. Registru centralizare consimțăminte

Acest document va fi de avut în vedere spre a fi aplicat mai ales dacă vă aflați într-unul din cazurile descrise în:

- Orientarea 3.5 cu privire la **posibilitatea de fotografiere, realizarea de capturi video și alte imagini** folosite în serviciul medical
- Orientarea 3.13 privitoare la **utilizarea datelor cu caracter personal în scopuri secundare** decât cele în care au fost colectate inițial
- Orientarea 3.16 privind **obținerea și gestionarea consimțământului persoanei vizate**

Mai exact, de fiecare dată când:

- Dorim să publicăm datele de identificare ale pacienților (ex. Fotografii, radiografii, buletine de analize medicale ș.a.) neanonimizate în cadrul cercetărilor științifice, articole, studii de specialitate;
- De fiecare dată când dorim să realizăm fotografii pacienților și să le publicăm pe blogul sau website-ul personal, în scop de promovare, publicitate, marketing;
- Atunci când dorim să obținem mărturii sau testimoniale din partea pacienților cu privire la serviciile medicale prestate și dorim să le afișăm în mediul online.

Model Declarație de consimțământ prelucrare date cu caracter personal

Prezenta declarație are ca scop solicitarea consimțământului persoanei vizate cu privire la colectarea, utilizarea, transferarea și protejarea datelor acesteia cu caracter personal.

(OPERATORUL - Clinica SRL / Medicul SRL / Medicul Persoană Fizică)_____ _____ prelucrează datele dvs. cu caracter personal în conformitate cu prevederile Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce

privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date, și de abrogare a Directivei nr. 95/46/CE ("Regulamentul general privind protecția datelor", în continuare "RGPD") și ale legislației naționale relevante în materia protecției datelor cu caracter personal.

Subsemnata/ul _____, în calitate de_____ în cadrul _____**(Operator)**, îmi exprim în mod liber consimțământul ca **(Operatorul)** să-mi prelucreze datele cu caracter personal, respectiv: numele și prenumele, data nașterii și localitatea de domiciliu, imaginea și vocea prin fotografii, video-uri, înregistrări audio, testimoniale, informații despre starea de sănătate, precum și experiența medicală a pacienților/cadrelor medicale în relaționarea cu **(Operatorul)** în scop de: informare, promovare, publicitate și în scop statistic și didactic/științific prin:

- Publicarea pe pagina oficială a **(Operatorului)**:_____ *(indicați expres)*
- Publicarea pe paginile de social media:
  - Facebook: _____ *(indicați expres)*
  - Instagram: _____ *(indicați expres)*
  - Twitter: _____*(indicați expres)*
  - Youtube: _____ etc.*(indicați expres)*
- Transmiterea către mass media în scopul publicității locale
- Publicarea în format tipărit

De asemenea, îmi exprim consimțământul ca datele să-mi fie prelucrate pe perioada necesară îndeplinirii scopurilor menționate mai sus și a obligațiilor legale care revin **(Operatorului)** respectiv, după caz, până la data retragerii consimțământului.

Confirm că am fost informat cu privire la următoarele:

- datele furnizate vor fi prelucrate de **(Operator)** conform cu prevederile din RGPD și nu vor fi transferate către terțe părți / vor fi transferate către: _____ (*de completat cu colaboratorii Societății cărora le transmiteți datele cu caracter personal, de exemplu: Societatea care se ocupă de mentenanța website-ului, de marketing, de serverele de stocare a datelor*)
- pot contacta persoana cu atribuții specifice protecției datelor sau managementului **(Operatorului)** la adresa de e-mail _____ cu privire la toate aspectele legate de prelucrarea datelor mele cu caracter personal.

Registru centralizare consimțăminte

DATA OBȚINERE CONSIMȚĂMÂNT	NUME / PRENUME PERSOANA VIZATĂ	E-MAIL PERSOANA VIZATĂ	DATE PRELUCRATE	SURSĂ DISTRIBUIRE / DIVULGARE DATE	TIP DE OBȚINERE CONSIMȚĂMÂNT	SOLICITARE DE ȘTERGERE	DATA ȘTERGERII	OBS.
15.06.2021	Gheorghe Manolescu	gheorghe.manolescu@yahoo.com	Adresa de email	Mail - Newsletter	Electronic	DA	15.09.2021	Dovada ștergerii se va păstra în dosarul de GDPR

ANEXA 5

Formularul tip Cerere de acces la datele cu caracter personal

Acest document va fi de avut în vedere spre a fi aplicat mai ales dacă vă aflați într-unul din cazurile descrise în:

- Orientarea 3.10 cu privire la **gestionarea cererilor persoanelor vizate** (pacienți / aparținători) cu privire la propriile informații
- Orientarea 3.11 cu privire la **gestionarea reclamațiilor angajaților respectiv pacienților**

Mai exact, de fiecare dată când:

- Cineva vrea să își execite un drept (de ștergere, de acces, de a fi informat) și vă solicită un formular, puteți să îi puneți la dispoziție documentul de mai jos.

!NB - Nici o persoană nu poate fi condiționată în exercitarea drepturilor sale de impunerea acestui formular. Acesta vă ajută să înțelegeți cât mai bine se poate solicitarea persoanei.

Model Cerere pentru exercitarea drepturilor persoanei vizate

În baza Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (în continuare "Regulamentul general privind protecția datelor" sau "RGPD"), a Legii nr. 190 din 18.07.2018 care reglementează măsurile necesare punerii în aplicare la nivel național a RGPD și a celorlalte dispoziții legale în materia protecției datelor cu caracter personal, aveți dreptul de a solicita din partea **Operatorului** _____ (în continuare "Societatea") accesul la datele dumneavoastră cu caracter personal, rectificarea sau ștergerea acestora sau restricționarea prelucrării, dreptul de a vă opune prelucrării în limitele și condițiile prevăzute de lege, precum și dreptul la portabilitatea datelor.

Vă informăm că prelucrarea datelor dumneavoastră colectate în baza formularului și documentelor atașate se va face exclusiv în scopul soluționării prezentei cereri.

I. Vă rugăm să completați datele dumneavoastră:
Nume:_____Prenume:_____
____CNP* _____(**acesta nu va fi colectat în mod implicit de fiecare dată, ci doar în situația în care operatorul constată că numele și prenumele nu este suficient, pentru a evita lărgirea bazei de date prin dublarea acestuia)*

II. În baza RGPD, solicitați exercitarea:

- dreptului de acces (Art. 15)
- dreptului la rectificare (Art. 16)
- dreptului la ștergerea datelor (Art. 17)
- dreptului la restricționarea prelucrării (Art. 18)
- dreptului la portabilitatea datelor (Art. 20)
- dreptului de opoziție (Art. 21)

III. În cazul în care în ultimele 12 luni ați depus o cerere având același obiect, vă rugăm precizați care este motivul noii solicitări _____
_____.

IV. Prin ce modalitate doriți să fiți contactat în cazul în care sunt necesare informații suplimentare? (este suficientă o singură opțiune)

- la următoarea adresă de e-mail: _____
- prin poștă, la adresa: _____
- la numărul de telefon:_____

V. Prin ce modalitate doriți transmiterea Răspunsului la cerere? (alegeți o singură opțiune)

- prin predare personală la sediul Societății
- prin poștă, la adresa: _____

Notă: nu ne asumăm responsabilitatea privind serviciile poștale.

- în format electronic, la următoarea adresă de e-mail: _____

Dacă optați pentru trimiterea informațiilor la adresa de e-mail indicată, vă asumați riscurile legate de comunicarea electronică de informaţii (interceptare, modificare, pierdere, distrugere, întârzieri în primirea datelor).

A se completa doar în cazul exercitării dreptului de acces (Art. 15 GDPR)
Vă rugăm să precizați informațiile sau activitățile de prelucrare la care face referire cererea dvs. (perioade de timp, date, nume sau tipuri de documente, orice referință de fișier și orice alte informații care ne pot permite să identificăm datele dumneavoastră):

_____

_____

A se completa doar în cazul exercitării dreptului la rectificare (Art. 16 RGPD)
Vă rugăm să precizați datele ale căror rectificare le solicitați și să anexați o dovadă în acest sens:

_____

_____

A se completa doar în cazul exercitării dreptului la ștergere (Art. 17 RGPD)
Vă rugăm să precizați datele ale căror ștergere le solicitați și motivul:

_____

_____

A se completa doar în cazul exercitării dreptului la restricționarea prelucrării (Art. 18 RGPD)
Vă rugăm să precizați motivul pentru care solicitați restricționarea prelucrării:

_____

_____

A se completa doar în cazul exercitării dreptului de opoziție (Art. 21)
Vă rugăm să precizați motivul pentru care vă exprimați opoziția la prelucrarea datelor dvs.

_____

_____

Confirm faptul că informațiile furnizate de mine prin prezenta cerere sunt reale şi corecte, în caz contrar fiind pasibil de sancțiune conform legii penale.

Dată: _____
Nume și prenume persoană vizată: _____
Semnătură persoană vizată: _____

ANEXA 6

Model de procedură de soluționare a cererilor persoanelor vizate

Acest document va fi de avut în vedere spre a fi aplicat mai ales dacă vă aflați într-unul din cazurile descrise în:

- Orientarea 3.10 cu privire la **gestionarea cererilor persoanelor vizate** (pacienți / aparținători) cu privire la propriile informații
- Orientarea 3.11 cu privire la **gestionarea reclamațiilor angajaților respectiv pacienților**

Mai exact, **puteți pune la dispoziție acest formular**, de fiecare dată când:

- Cineva vrea să își execite un drept (de ștergere, de acces, de a fi informat) și vă solicită un formular
- Cineva vă depune o reclamație specifică protecției datelor cu caracter personal
- Este efectuat un control din partea A.N.S.P.D.C.P.
- Partenerii de afaceri (colaboratorii) doresc să se asigure că sunteți în conformitate cu reglementările R.G.P.D.

Procedură de soluționare a cererilor persoanelor vizate

Această procedură poate fi adoptată la nivel intern și urmărită astfel:

- **Primirea cererii**: O cerere de acces la datele cu caracter personal este primită fie de conducerea organizației, fie de persoana cu atribuții în domeniul protecției datelor, cum ar fi Responsabilul cu Protecția Datelor (DPO) sau chiar de către secretariatul unității medicale.

- **Verificarea și analiza cererii**: Cererea este analizată pentru a se stabili natura și amploarea acesteia. Se face o verificare privind identitatea solicitantului și se identifică datele cu caracter personal în cauză (spre exemplu, ne asigurăm că cel care ne solicită informațiile proprii prin email este și persoana îndreptățită să le primească. *SherlockHolmes@gmail.com* vă scrie un mesaj că dorește să primească rezultatele analizelor medicale proprii, identificându-se ca Ion Georgescu).

Se evaluează dacă organizația prelucrează aceste date și dacă solicitantul are dreptul de a face cererea. Pot fi necesare informații suplimentare din partea solicitantului pentru a clarifica cererea, cum ar fi date din cartea de identitate pentru a putea valida identitatea ș.a.

- **Decizia de prelungire a termenului de soluționare**: În cazul în care cererea este complexă și necesită mai mult timp pentru a fi soluționată, se poate decide prelungirea termenului de soluționare a cererii cu încă o lună. Solicitantul este informat despre această prelungire în cel mai scurt timp.

- **Răspunsul la cerere**: În funcție de analiza efectuată, organizația răspunde la cerere conform formularului tipizat corespunzător situației:
    - **Varianta I**: Se confirmă faptul că organizația prelucrează datele cu caracter personal ale solicitantului și i se furnizează o copie a acestor date și informații privind prelucrarea lor.
    - **Varianta II**: Dacă organizația nu deține suficiente informații la care face referire solicitantul, acesta este rugat să furnizeze date suplimentare.
    - **Varianta III**: În cazul în care cererea este complexă și necesită mai mult timp pentru a fi soluționată, se informează solicitantul înăuntrul termenului de soluționare a cererii că acesta va fi prelungit cu încă o lună.

- **Transmiterea răspunsului:** Răspunsul este trimis solicitantului în format scris, semnat de conducerea organizației și de persoana cu atribuții în domeniul protecției datelor. Răspunsul poate fi transmis fie la adresa de corespondență indicată de solicitant, fie în format electronic, la adresa de e-mail indicată de acesta.

- **Arhivarea comunicării**: După furnizarea răspunsului solicitat, cererea va fi considerată a fi soluționată, urmând a fi arhivată împreună cu Răspunsul și Anexele specifice atașate, pentru o perioadă de 3 ani.

NB! Acesta este un exemplu de procedură operațională de gestionare a cererilor de acces la datele cu caracter personal, care poate fi adaptată pentru un spital, o clinică sau un cabinet de medicină individuală.

Vă reamintim că procedura trebuie să fie revizuită și adaptată în conformitate cu specificul activității dumneavoastră.

ANEXA 7

Modele de formulare de răspuns la cererile persoanei vizate

Acest document va fi de avut în vedere spre a fi aplicat mai ales dacă vă aflați într-unul din cazurile descrise în:

- Orientarea 3.10 cu privire la **gestionarea cererilor persoanelor vizate** (pacienți / aparținători) cu privire la propriile informații
- Orientarea 3.11 cu privire la **gestionarea reclamațiilor angajaților respectiv pacienților**

Mai exact, de fiecare dată când:

- Cineva și-a exercitat un drept, ați urmărit procedura de soluționare a cererilor, plângerilor sau reclamațiilor și doriți să formulați un răspuns

Puteți să vă folosiți de unul din formularele de răspuns de mai jos pentru cazurile de: **solicitări de acces la date, de informare asupra datelor prelucrate sau de ștergere, restricționare sau opoziție la prelucrările de date**.

Formular tip pentru Răspunsul la cererea privind accesul la datele cu caracter personal

Către_____ *(Numele şi prenumele solicitantului)*

Stimată doamnă / Stimate domnule_____

În urma cererii dumneavoastră nr. _____ din data de_____ prin care, în temeiul art. 15 din Regulamentul 2016/679 al Parlamentului European privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date ați solicitat accesul la datele cu caracter personal,

Varianta I
Vă confirmăm că _____ *(numele operatorului - clinicii - spitalului - medic SRL)* prelucrează date cu caracter personal și ca urmare, vă trimitem anexate următoarele documente:

- copie a datelor care se prelucrează – Anexa nr.1
- informații privind prelucrarea acestor date – Anexa nr.2

Varianta II
Vă informăm că pentru rezolvarea cererii dumneavoastră, întrucât_____ *(numele operatorului - clinicii - spitalului - medic SRL)* nu deţine suficiente informaţii la care faceţi referire, să reveniți cu următoarele date suplimentare:

_____

_____

Varianta III
Vă informăm că, având în vedere numărul mare de solicitări și complexitatea acestora, termenul de soluționare inițial de o lună a cererii dumneavoastră, se va prelungi cu încă un termen de o lună.

Data _____
_____ (semnătură conducere)
_____(semnătură Responsabil cu protecția datelor - dacă există)

Formular tip pentru Informarea persoanei vizate cu privire la prelucrarea datelor cu caracter personal

Stimată doamnă / Stimate domnule_____

În urma cererii dumneavoastră nr. _____/_____ prin care solicitați informarea cu privire la datele cu caracter personal prelucrate de *(numele operatorului - clinicii - spitalului - medic SRL)*, vă transmitem următoarele informații:

I. Date de identificare operator:
Denumire operator:_____
Sediul:_____
Cod unic de înregistrare:_____
Date contact:_____

II. Scopul prelucrării datelor personale ale dumneavoastră este reprezentat de:

_____

_____acest lucru fiind realizat în baza (temeiul juridic - art. 6 alin. 1 lit a-f - selectați care este aplicabil)

_____

III. Categoriile de date cu caracter personal prelucrate sunt următoarele:

_____

_____

IV. Datele personale ale dumneavoastră sunt transmise următorilor destinatari:

_____

_____

V. Perioada pentru care vor fi stocate datele personale ale dumneavoastră este de (se completează doar în măsura în care este posibil) _____

VI. În baza Regulamentului (UE) nr. 679 din 27 aprilie 2016 al Parlamentului European și al Consiliului privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date, aveți următoarele drepturi: dreptul de rectificare a datelor, dreptul la ștergere a datelor, dreptul de restricționare a datelor, dreptul la opoziție, precum și dreptul de a depune o plângere în fața Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP).

VII. Sursa colectării datelor personale ale dumneavoastră este reprezentată de:

_____

_____

Informațiile și documentele solicitate v-au fost furnizate la următoarea adresă de corespondență: _____/ în format electronic, la următoarea adresă de e-mail: _____

Data _____

_____ (semnătură conducere)

_____(semnătură Responsabil cu protecția datelor - dacă există)

Formular tip pentru Răspuns la cererea nr._____/_____ privind exercitarea dreptului _____

Stimată doamnă / Stimate domnule_____

În urma cererii dumneavoastră nr. _____/_____ prin care solicitați ștergerea / portabilitatea / restricționarea datelor cu caracter personal prelucrate de (*numele operatorului - clinicii - spitalului - medic SRL)*, vă transmitem următoarele:

Varianta I
Cererea dumneavoastră a fost respinsă întrucât:
_____
_____
_____

Varianta II
Cererea dumneavoastră a soluționată și au fost întreprinse următoarele măsuri:
_____
_____
_____

Prezentul răspuns a fost transmis la următoarea adresă de corespondență: _____/ în format electronic, la următoarea adresă de e-mail: _____.

Data _____
_____ (semnătură conducere)
_____(semnătură Responsabil cu protecția datelor - dacă există)

ANEXA 8

Procedura privind managementul incidentelor de securitate

Acest document va fi de avut în vedere spre a fi aplicat mai ales dacă vă aflați într-unul din cazurile descrise în:

- Orientarea 3.12 privind **modalitatea de răspuns în caz de încălcare a securității și confidențialității datelor** pacientului sau a altei persoane vizate

Mai exact, de fiecare dată când:

- S-au pierdut date, au fost furate, au fost divulgate în mod neautorizat
- S-au distrus date de pe suporturi electronice
- Am suferit un atac cibernetic care au blocat temporar datele, etc.

Procedură privind managementul incidentelor de securitate

I. Descrierea Procedurii

I.1. Identificarea tipului de încălcare a securității datelor

Regulamentul stabileşte trei categorii de încălcări ale securităţii datelor cu caracter personal:

- **încălcarea confidenţialităţii** - în cazul în care se produce divulgarea neautorizată sau accidentală a datelor cu caracter personal sau accesul la acestea
- **încălcarea integrităţii** - în cazul în care se produce o modificare neautorizată sau accidentală a datelor cu caracter personal
- **încălcarea disponibilităţii** - în cazul în care se produce o pierdere neautorizată sau accidentală a accesului la date sau distrugerea datelor cu caracter personal

[Operatorul] face toate eforturile pentru a preveni încălcarea securităţii datelor cu caracter personal. Totuşi, este posibilă producerea unei erori sau unor evenimente care nu se află sub controlul **[Operatorul]**.

Încălcările securităţii datelor cu caracter personal se pot produce din mai multe cauze, printre care se numără și:

- pierderea sau furtul de date sau echipamente pe care sunt stocate datele (chiar dacă dispozitivul este criptat trebuie să se acorde atenţie dacă există un back-up disponibil)
- control inadecvat al accesului, care permite utilizarea neautorizată
- erori ale echipamentelor utilizate
- dezvăluirea neautorizată (de exemplu, un e-mail trimis către un destinatar incorect sau un document trimis la o adresă greşită, etc.)
- erori umane ale persoanelor care se ocupă de activitățile de prelucrare
- evenimente neprevăzute, precum incendiile sau inundaţiile
- atac cibernetic

Consecinţele unei încălcări a securităţii datelor cu caracter personal pot cauza prejudicii materiale sau morale **pentru persoanele vizate**, cum ar fi pierderea controlului asupra datelor cu caracter personal, furtul de identitate, fraudă, pierderi financiare, afectarea reputaţiei sau orice alt dezavantaj economic sau social pentru persoana vizată în cauză.

Consecinţele unei încălcări a securităţii datelor cu caracter personal **pentru [Operatorul]** includ afectarea reputaţiei şi riscurile financiare, în special în ceea ce priveşte eventualele amenzi care pot fi impuse de autoritatea de supraveghere şi despăgubirile care pot fi solicitate de persoanele vizate ale cărori drepturi au fost încălcate.

I.2. Constatarea unui incident de securitate

Oricare membru al personalului **[Operatorul]** sau altă persoană care descoperă o încălcare a securităţii datelor cu caracter personal sau crede că a avut loc o încălcare a securităţii datelor cu caracter personal, este obligată să o raporteze imediat Responsabilului cu protecția datelor sau conducerii unității medicale.

Datele de contact ale Responsabilului cu protecţia datelor din cadrul **[Operatorul]** sunt următoarele: e-mail: dpo@_____.ro

La anunţarea incidentului, persoana care îl raportează trebuie să furnizeze, în măsura în care este posibil, următoarele informații:

- natura încălcării descoperite
- gravitatea și amploarea încălcării

- categoriile de date vizate de încălcare
- numărul de persoane vizate afectate
- persoanele ce au avut acces la datele respective
- măsurile dispuse pentru limitarea efectelor încălcării

I.3. Investigarea incidentului

După ce a fost informat cu privire la un incident privind securitatea datelor, Responsabilul cu protecţia datelor, persoana cu atribuții sau conducerea, va întreprinde o scurtă investigaţie pentru a stabili dacă incidentul se confirmă sau nu.

Astfel, persoana care realizează investigația, va solicita furnizarea de detalii suplimentare părților care pot oferi aceste detalii, în termen de 24 de ore de la descoperirea încălcării, referitoare la:

- natura presupusei încălcări, inclusiv tipurile de date care au fost compromise şi modul în care se crede că a avut loc încălcarea potenţială a datelor
- cine este sau poate fi afectat, inclusiv numărul estimativ de persoane
- consecinţele încălcării şi ce măsuri pot fi luate sau care au fost luate pentru a diminua consecinţele încălcării

I.4. Informare şi notificare

Responsabilul cu protecţia datelor, persoana cu atribuții sau conducerea va fi responsabil(ă) de evaluarea încălcării şi de a recomanda Managementului decizia de a notifica încălcarea către autoritatea de supraveghere, în termen de 72 de ore de la momentul confirmării incidentului, pe *www.dataprotection.ro - https://www.dataprotection.ro/formulare/formularBresaGdpr.do?action=view_action&newFormular=true.*

Se va evalua totodată, dacă persoanele vizate trebuie să fie informate despre încălcare, iar dacă se constată necesar, se vor informa și persoanele vizate.

Responsabilul cu protecţia datelor sau persoana cu atribuții specifice, poate contacta, după cum este necesar, Secretariatul **[Operatorul]**, Poliţia dacă a existat o activitate ilegală, Managementul dacă este probabil să existe interes pentru presă, colaboratori IT&C dacă încălcarea implică şi securitatea IT, alte departamente, după caz. De asemenea, pot exista cerinţe legale sau contractuale de notificare.

I.5. Limitarea consecinţelor şi recuperarea

Persoanele însărcinate cu soluționarea incidentului privind securitatea datelor trebuie să ia cât mai curând posibil măsuri pentru a recupera pierderile şi limitarea daunele. Paşii sunt următorii:

- încercarea de recuperare a echipamentului pierdut
- încercarea de a restabili controlul asupra datelor personale, de exemplu rechemarea e-mail-urilor, eliminarea datelor de pe website-uri etc.
- utilizarea copiilor de siguranţă pentru a recupera datele pierdute, deteriorate sau furate, schimbarea parolelor relevante cât mai curând posibil
- dacă au fost pierdute / furate date bancare, contactarea directă a băncilor pentru sfaturi privind prevenirea utilizării frauduloase

I.6. Evaluare şi răspuns

Odată ce incidentul a fost ţinut sub control, persoanele însărcinate cu soluționarea incidentului trebuie să efectueze o analiză a cauzelor încălcării şi a eficacităţii răspunsului. Analiza trebuie să ia în considerare tipul de date, ce măsuri de protecţie au fost în vigoare (ex. criptarea), ce s-a întâmplat cu datele şi dacă ar putea exista consecinţe mai mari ale încălcării.

Dacă se identifică probleme în curs, atunci trebuie elaborat un **plan de acţiune** pentru a le pune în aplicare. În cazul celor mai grave încălcări, un raport va fi prezentat conducerii **[Operatorul]**.

Responsabilul cu protecţia datelor sau managementul unităţii medicale va ţine un **Registru de evidenţă a tuturor incidentelor** (excel) privind încălcarea confidenţialităţii datelor, inclusiv a acţiunilor întreprinse pentru a diminua consecinţele încălcării şi lecţiile învăţate.

Model Registru de evidență a incidentelor de securitate

Nr.	Tipul incidentului și modul în care a avut loc acesta	Caracterul încălcării securității datelor	Natura și conținutul datelor afectate de incident	Data și ora descoperirii	Data și ora survenirii	Persoana care a descoperit incidentul	Persoana responsabilă de domeniul în care a survenit incidentul	Gradul de probabilitate privind afectarea drepturilor persoanelor vizate	Măsurile luate anterior pentru prevenirea unui astfel de incident	Măsurile luate pentru a opri incidentul / ameliora situația	Necesitatea de a comunica incidentul Autorității Naționale / Persoanelor vizate	Numărul aproximativ și categoriile persoanelor vizate afectate	Consecințele probabile ale incidentului
1	Pierderea unui caiet (tip registru) care conținea numele, prenumele, numărul de telefon a 49 pontențiali clienți	Confidențialitate	Nume, prenume, oraș, telefon, sumă dorită, modalitate contract, observații	17.08.2022 ora 14:55	17.08.2022 ora 8:35	Angajatul operatorului cu atribuții specific pentru completarea registrului (caietului)	Managementul operatorului	Mic	1.Responsabilizarea angajaților prin menționarea unor prevederi cu titlu general în documente precum - Procedura de arhivare a documentelor, Regulamentul intern, convenția de confidențialitate semnată. 2. Scanarea documentului 3. Aprobarea unui plan de reacție la incidentele de securitate	Demararea unei investigații interne cu privire la incident. Contactare a firmei de curățenie / a celei de colectare a deșeurilor pentru încercarea de recuperare a documentelor. Informarea Responsabilului cu Protecția Datelor cu privire la incident.	Nu se impune, poate fi notificat dacă se decide în acest sens de către management	49 potențiali clienți ai operatorului	Contactarea persoanelor vizate în afara unui temei legal de către o persoană care recuperează părți din registru.

Calculul riscului

Informatii relevante	Proprietarii datelor	Tipul datelor	Detaliile riscului produs (Amenințări la confidențialitate, integritate, disponibilitate)	NOTĂ PROBABILITATE (1 - Mică, 10 - Mare)	NOTĂ GRAVITATE (1 - Mică, 10 - Mare)	SCORUL AMENINȚĂRII (2 - Mică, 20 - Mare)	Tratarea riscului (Tratează, Evită, Transferă sau Acceptă)	Data propusă pentru remedierea riscului	Data completării tabelului	Responsabilul riscului
				0	0	0				
				0	0	0				
				0	0	0				
				0	0	0				

Graficul riscurilor

		Impactul unui risc	Foarte mic	Mic	Mediu	Mare	Foarte mare
			ACCEPTABIL Efecte minime spre deloc		TOLERABIL Efectele sunt resimțite dar fără un rezultat critic	INDEZIRABIL Consecințe serioase asupra drepturilor persoanei vizate	INTOLERABIL Poate apărea un eveniment major (dezastru)
Probabilitatea producerii riscului	IMPROBABIL Este puțin posibil să apară riscul	Foarte mică	1	2	4	5	4
		Mică	2	3	5	6	7
	POSIBIL Este posibil ca riscul să apară	Medie	4	5	6	7	8
		Mare	5	6	7	8	9
	PROBABIL Riscul va apărea	Foarte mare	6	7	8	9	10