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.