# 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*