# 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*