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*