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*