3.1 ORIENTĂRI PRIVIND ACORDURILE DE CONFIDENȚIALITATE ȘI CONTRACTELE DE SERVICII ÎNCHEIATE CU MEDICII ANGAJAȚI SAU COLABORATORI

- Enumerarea unor elemente cheie care trebuie incluse la nivelul contractelor prin care se prelucrează date cu caracter personal
- Prezentarea riscurilor neluării măsurilor organizatorice de actualizare a contractelor
- Prezentarea clauzelor contractuale model

În desfășurarea activității profesionale, medicii și personalul medical interacționează cu o varietate de parteneri cu care furnizorul de servicii medicale, adică operatorul (cabinetul medical, clinica, unitatea spitalicească, entitatea de îngrijiri medicale organizată sub orice formă) are încheiate sau va încheia contracte de furnizare de servicii.

În acest context, operatorul care va face prelucrări de date cu caracter personal necesare executării viitoarelor contracte de servicii este cel care **își alege parteneri prin care să desfășoare aceste activități** precum: *curierat, reparații laptopuri sau telefoane, mentenanță infrastructură informatică, mentenanță sistem de supraveghere video, contracte de colaborare cu alți medici, specialiști sau diverse laboratoare cărora li se trimit informații care pot cuprinde date cu caracter personal.*

În virtutea **principiului responsabilității operatorului** acesta trebuie să ia toate măsurile necesare pentru a se asigura că **atât personalul propriu cât și partenerul asigură un nivel înalt de securitate și confidențialitate a datelor!**

Clauze de asigurare a confidențialității și securității datelor

Pentru a se asigura de cele menționate anterior este recomandat ca operatorul să ia măsuri precum cele referitoare la:

- **Identificarea datelor cu caracter personal prelucrate de către angajat, respectiv de către partener**
  Exemplu: o firmă de curierat care a contractat serviciile unei clinici medicale sau ale unui laborator de recoltare a probelor biologice, în serviciul prestat, va stoca temporar buletinele de analiză transmise dintr-o locație în alta. Neasigurarea unui cadru de securitate și confidențialitate a acestui proces poate atrage sancțiuni clinicii. Există sancțiuni aplicate în România pentru lipsa selectării unui furnizor de servicii specializat care oferă un nivel ridicat de protecție în cadrul transferurilor pe care le efectuează. Această lipsă de responsabilitate a dus la următoarea situație: șoferul mașinii care transportă pachetul clinicii intuiește că în acesta pot fi și bani, deschide pachetul, ia banii, însă fără să vrea compromite probele biologice.

- **Identificarea scopurilor și naturii prelucrării**
  Exemplu: O firmă de dezvoltare soft oferă mentenanță unei aplicații informatice în care sunt introduse datele pacientului – scopul acestui acces este pentru a remedia eventualele probleme.

- **Identificarea temeiurilor legale, duratei prelucrării dar și măsurilor necesare pentru a proteja datele**
  Exemplu: Un medic colaborator va prelucra în baza contractului avut cu clinica medicală, datele pacienților. Acesta va avea acces la o multitudine de date medicale pe care le va introduce într-un sistem. Acestuia i se creează o adresă de email profesională – a clinicii – de pe care poartă conversația. La încetarea colaborării, întregul acces va fi retras. Pentru a prelucra datele, medicul se obligă contractual să nu divulge și să nu folosească toate aceste date în scopuri secundare.

- **Consecințele care pot apărea în cazul nerespectării obligațiilor contractuale asumate**
  Exemplu: Divulgarea datelor în cazul de mai sus, furtul bazei de date sau

folosirea în alte scopuri poate plasa medicul într-o zonă de nelegalitate și astfel să atragă asupra sa sancțiuni în cazul apariției unei investigații.

Pentru a ajuta medicii care administrează cabinete individuale medicale, ori clinici respectiv laboratoare medicale, vă punem la dispoziție:

- un model de clauze care ar trebui preluate în relație cu angajații (**Anexa nr.1 - Model de clauze care ar trebui preluate în relație cu angajații**)

- un model de acord de confidențialitate pe care să îl utilizați în relație cu colaboratorii persoane împuternicite, cu furnizorii de servicii sau cu cei care acționează în numele și pe seama operatorului (**Anexa nr.2 - Model de acord de confidențialitate pe care să îl utilizați în relație cu colaboratorii PÎ**).

Ce ar trebui să cunoașteți în calitate de administrator al unui S.R.L. respectiv al altei forme juridice de organizare a profesiei:

Înainte de a încheia un contract cu un furnizor de servicii extern (ex: servicii de arhivare, de distrugere a documentelor, de traduceri) sau un colaborator (ex: medic care prestează servicii în baza unui contract) trebuie să ne asigurăm că:

- Măsurile de confidențialitate și securitate a datelor luate de către furnizor sau de către medic sunt cel puțin la fel de ridicate ca cele luate de către cabinet / spital

La întocmirea contractului, în completarea aspectelor de mai sus, este bine să ținem cont de:

- Tipologia de acțiuni permise
- Procedurile specifice prin care se poate avea acces la date – spre exemplu să nu lucreze cu subcontractori decât cu acceptul scris al operatorului
- Să notifice operatorul în cazul în care anumite date au fost pierdute, furate, utilizate sau accesate în mod neautorizat
- Să raporteze în cel mai scurt timp orice încălcare la adresa confidențialității sau securității datelor
- Să returneze datele sau să le distrugă de îndată ce se încheie contractul (ex: orice fel de documente originale sau copii să fie predate operatorului, toate dispozitivele mobile să fie returnate ș.a.)

Cazuistică relevantă

O rea practică în acest context ar fi aceea în care un angajat al clinicii medicale (ex. un asistent medical) folosește accesul la datele cu caracter personal ale pacienților pentru a le vinde unui terț (ex. o companie de marketing farmaceutic). Această acțiune ar încălca normele de confidențialitate și securitate a datelor, precum și obligațiile contractuale asumate de angajat.

Medicover SRL – o persoană a trimis unui client un email care conținea actele adiționale ale contractelor de prestări servicii medicale care aparțineau altor clienți ai operatorului. Astfel au fost divulgate date precum: nume, prenume, CNP, adresă, semnătură. Amenda aplicată a fost de 1000 €.

(https://www.dataprotection.ro/?page=Comunicat_Presa_24_11_2022&lang=ro)