



**UNIVERSITATEA DE MEDICINĂ ȘI FARMACIE  
„VICTOR BABEȘ” DIN TIMIȘOARA**

**MANAGEMENTUL COMUNICĂRII ÎN PRACTICA MEDICALĂ  
SUPOORT DE CURS PENTRU PROGRAMUL UNIVERSITAR DE  
MASTERAT RESPONSABILITATEA JURIDICĂ A PERSONALULUI  
MEDICAL**

**Prof.univ.dr. Ramona Amina POPOVICI**

## GDPR ÎN SISTEMUL DE SĂNĂTATE

- unul dintre cele mai dezbătute acte legislative ale Uniunii Europene este **Regulamentul UE 2016/679**, cunoscut și sub denumirea de **„Regulament general privind protecția datelor”** sau **„GDPR”**
- prezentul Regulament stabilește normele referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, precum și normele referitoare la libera circulație a datelor cu caracter personal
- Regulamentul UE 2016/679 înlocuiește Directiva anterioară în materie, **Directiva 95/46/CE**
- Regulamentul general privind protecția *datelor* sau *GDPR* este aplicabil începând cu data de **25 mai 2018**
- potrivit art. 21 din Legea nr. 46/2003 privind drepturile pacientului, "toate informațiile privind starea pacientului, rezultatele investigațiilor, diagnosticul, prognosticul, tratamentul, datele personale **sunt confidențiale chiar și după decesul acestuia**"
- potrivit art. 9 din cuprinsul Regulamentului (GDPR) "Se interzice prelucrarea de date cu caracter personal care dezvăluie, originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea de date genetice, **de date privind sănătatea** sau de date privind viața sexuală sau orientarea sexuală a unei persoane fizice
- odată cu intrarea în vigoare a Regulamentului General privind protecția datelor cu caracter personal, siguranța prelucrării și stocării datelor din domeniul medical va reprezenta o mare responsabilitate pentru furnizorii de servicii medicale
- Regulamentul se adresează și trebuie respectat atât de către personalul medical care își exercită profesia în sistemului medical privat, cât și în sistemului medical de stat
- Regulamentul trebuie să fie respectat de către medici, tehnicienii dentari, personalul tehnico - administrativ din spitale, producătorii de medicamente, furnizorii de medicamente și produse medicale, dar și de către administratorii cabinetelor medicale private

**Prelucrarea datelor cu caracter personal** reprezintă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal:

- *colectarea*
- *înregistrarea*
- *organizarea*
- *stocarea*
- *adaptarea sau modificarea*
- *extragerea*
- *utilizarea*
- *transmiterea*
- *ștergerea*
- *restricționarea*

- potrivit art. 22 din Legea nr. 46/2003 privind drepturile pacientului, "Informațiile cu caracter confidențial pot fi furnizate numai în cazul în care *pacientul își dă consimțământul explicit* sau dacă *legea o cere în mod expres*"

- potrivit art. 23 din Legea nr. 46/2003 privind drepturile pacientului, "în cazul în care informațiile sunt necesare altor furnizori de servicii medicale acreditați, implicați în tratamentul pacientului, ***acordarea consimțământului nu mai este obligatorie***"

- ***a nu se confunda*** acordul pentru actul medical cu acordul pentru prelucrarea datelor cu caracter personal

- acordul pacientului pentru actul medical nu are legătură cu prelucrarea datelor cu caracter personal, prelucrarea datelor realizându-se chiar dacă actul medical în sine nu a avut loc (***invers nu***)

- consimțământul pacientului pentru prelucrarea datelor sale cu caracter personal trebuie separat de consimțământul (acordul) acestuia pentru acordarea îngrijirilor de sănătate

- în procesul prelucrării datelor cu caracter personal ale pacienților, medicul împreună cu întreg personalul medical trebuie să respecte o serie de obligații pentru ca acea prelucrare să fie realizată conform dispozițiilor legale

❖ *Obligațiile medicului privind prelucrarea datelor personale ale pacienților*

- ✓ informarea pacienților
- ✓ stabilirea perioadelor de stocare a datelor în funcție de scop și ștergerea datelor care depășesc durata
- ✓ verificarea furnizorilor care au acces la datele pacienților
- ✓ aplicarea măsurilor adecvate de securitate
- ✓ păstrarea unui registru al activităților de prelucrare a datelor
- ✓ limitarea datelor colectate la cele strict necesare și folosirea acestora doar conform scopurilor definite și incluse în informare

❖ *Informarea pacienților*

- informarea este obligatorie atunci când datele sunt obținute direct de la pacient
- informarea trebuie făcută **înainte** de colectarea datelor
- informarea pacientului trebuie să conțină o serie de date și informații ( *numele și datele de contact ale operatorului; ce date vor fi prelucrate; scopul prelucrării și temeiul legal, categoriile de destinatari; durata de păstrare a datelor, drepturile persoanei vizate*)

❖ *Alte date ce pot fi incluse în informare*

- ☐ posibilitatea retragerii consimțământului
- ☐ dacă este cazul, utilizarea ulterioară a datelor în alt scop decât cel pentru care au fost colectate datele (ex: un medic dorește să utilizeze datele în scop de cercetare)

- datele cu caracter personal ale pacienților pe care personalul medical le colectează nu trebuie să cuprindă informații care nu au nicio legătură cu obiectul consultației sau care nu sunt esențiale pentru tratarea și îngrijirea acestuia (ex: religia pacientului sau orientarea sexuală)
- nu trebuie colectate mai multe date decât este necesar în fiecare caz
- datele pe care personalul medical le colectează și le transferă în dosarele pacienților trebuie să fie adecvate, relevante și limitate la ceea ce este necesar pentru îngrijirea pacientului prin activități de prevenire, de diagnostic și îngrijire

❖ *Date colectate de regulă*

- datele de identificare
- numărul cardului de sănătate
- istoricul medical
- istoricul tratamentelor
- diagnosticele medicale

❖ *Date necesare doar uneori (doar când este necesar)*

- situația familială (starea civilă, numărul copiilor)
- viața profesională (profesia, condițiile de muncă)
- obiceiurile de viață, alimentare

❖ *Date care de regulă nu sunt necesare*

- religia
- opinii politice
- originea etnică

- spre deosebire de dosarele pacienților, care justifică o durată de păstrare destul de îndelungată, datele legate de programări pot fi șterse mult mai repede, fiind greu de crezut că se justifică o perioadă mai mare de un an
- încălcarea securității datelor duce în mod inevitabil la distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la aceste date
- personalul administrativ din cabinetul medical nu trebuie să aibă acces global la dosarele pacienților, ci doar la acele date care sunt necesare funcțiilor lor
- există o serie de principii care trebuie respectate cu privire la prelucrarea datelor personale ale pacienților

### ***Principiile prelucrării datelor cu caracter personal***

- ❖ *prelucrarea datelor în mod legal, echitabil și transparent față de persoana vizată*
  - ❖ *colectarea datelor în scopuri determinate, explicite și legitime*
  - ❖ *păstrarea datelor exclusiv pe perioada de timp necesară îndeplinirii scopurilor pentru care au fost prelucrate*
  - ❖ *prelucrarea datelor într-un mod care asigură securitatea adecvată a datelor cu caracter personal*
  - ❖ *exactitatea datelor cu caracter personal*
- orice prelucrare de date cu caracter personal poate fi efectuată numai dacă pacientul și-a exprimat consimțământul în mod ***expres și neechivoc*** pentru acea prelucrare
  - exprimarea consimțământului de către persoana vizată reprezintă "orice manifestare de voință ***liberă, specifică, informată și lipsită de ambiguitate*** prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate"
  - consimțământul pacientului nu este exprimat în mod liber în situația în care este afectat de vicii de consimțământ (***eroare, dol, violență, leziune***)
  - consimțământul trebuie să fie unul specific
  - un consimțământ foarte larg, dat pentru scopuri generale/ nedeterminate nu este valid

- dacă prelucrarea datelor se face în mai multe scopuri, consimțământul trebuie exprimat pentru toate scopurile prelucrării
- potrivit articolului 7 alin. (3) din Regulamentul general privind protecția datelor cu caracter personal, orice persoană are *dreptul să își retragă în orice moment consimțământul*
- înainte de a-și exprima consimțământul, pacientul trebuie să fie informat de către personalul medical cu privire la faptul că are dreptul de a-și retrage acest consimțământ
- retragerea consimțământului nu afectează legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia

❖ *Drepturile pacienților privind datele cu caracter personal*

- pot accesa propriile lor date cu caracter personal
  - pot obține rectificarea datelor cu caracter personal inexacte
  - pot obține completarea datelor cu caracter personal care sunt incomplete
  - pot cere ștergerea datelor cu caracter personal în anumite situații speciale
- pacienții pot cere ștergerea datelor cu caracter personal atunci când datele nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate sau atunci când acestea au fost prelucrate ilegal
- potrivit noului Regulament privind protecția datelor cu caracter personal, este instituit un regim sancționator mult mai sever decât cel instituit anterior, pentru acele situații în care cei care prelucrează datele cu caracter personal ale persoanelor fizice nu respect prevederile acestui act normativ
- stabilirea unor *amenzi administrative de până la 20.000.000 EUR* sau de *până la 4% din cifra de afaceri* globală totală anuală

***Prelucrarea datelor cu caracter personal se poate realiza atunci când aceasta este necesară în următoarele scopuri***

❖ *medicina preventivă*

- ❖ *medicina muncii*
- ❖ *evaluarea capacității de muncă a angajatului*
- ❖ *stabilirea unui diagnostic medical*
- ❖ *furnizarea de asistență medicală sau socială*
- ❖ *gestionarea sistemelor și serviciilor de sănătate sau de asistență socială*

- datele speciale cu caracter personal pot fi prelucrate în scopuri legate de ***medicina preventivă*** sau ***a muncii*** în cazul în care datele respective sunt prelucrate de către un profesionist supus obligației de păstrare a secretului profesional sau sub responsabilitatea acestuia sau de o altă persoană supusă, de asemenea, unei obligații de confidențialitate

- în România există ***Legea nr. 677/2001*** cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, doar că Regulamentul este un act juridic superior Legii nr. 677/2001

- Legea nr. 677/2001 prevede o sancțiune mult mai mică decât cea reglementată în cadrul GDPR-ului

- Legea nr. 677/2001 prevede o amendă maximă de 50.000 de lei

- Regulamentul (GDPR) a fost emis în anul 2016, dar a fost acordat un termen de 2 ani de zile până la aplicarea lui efectivă pentru ca operatorii de date cu caracter personal să aibă timp să se conformeze acestor prevederi

- Regulamentele sunt acte normative ale Uniunii Europene care au forță juridică obligatorie în fiecare stat membru

- Regulamentul intră în vigoare în același timp în toate statele membre

- *Directiva 95/46/CE (nu mai este în vigoare acum, fiind înlocuită de GDPR)*

- spre deosebire de Regulamente, Directivele stabilesc o direcție, stabilesc anumite rezultate care trebuie realizate, dar fiecare stat membru trebuie să transpună textul Directivei în legislația națională



- pentru ca o Directivă să intre în vigoare este nevoie ca ea să fie transpusă într-o lege națională, care lege să fie apoi adoptată de Parlamentul țării în cauză
- operatorul nu poate schimba scopul pentru care au fost colectate datele, fără informarea prealabilă a persoanei vizate și parcurgerea tuturor pașilor tranzitorii necesari, atunci când este cazul (obținerea unui nou consimțământ pentru noua prelucrare a datelor)
- amendarea Spitalului Haga pentru neasigurarea securității dosarelor pacienților săi
- o persoană foarte cunoscută în Olanda a fost pacienta spitalului din Haga, prilej cu care zeci de angajați ai spitalului, mânați de o curiozitate mistuitoare, au studiat dosarul medical al pacientului, fără a avea un motiv real pentru a face asta
- în urma investigației, a fost impusă Spitalului Haga o amendă de 460.000 de euro pentru neasigurarea unui grad adecvat de securitate al datelor
- pe lângă această amendă, spitalul din Haga a riscat o nouă sancțiune
- pentru a determina spitalul să îmbunătățească securitatea datelor pacienților, Autoritatea de supraveghere olandeză a impus, pe lângă amenda menționată mai devreme, o comandă, sau mai bine spus o obligație, supusă și aceasta unei pedepse în cazul în care nu va fi îndeplinită
- dacă Spitalul Haga nu reușește să îmbucățească securitatea datelor pacienților până la data de 2 octombrie 2019, spitalul va trebui să plătească 100.000 EUR pentru fiecare două săptămâni de întârziere, până la un maxim de 300.000 EUR
- în octombrie 2018, Spitalul Barreiro din Portugalia a fost amendat cu 400.000 de euro pentru incapacitatea de a asigura confidențialitatea și integritatea datelor (securitatea datelor)
- Autoritatea portugheză pentru protecția datelor a concluzionat că personalul spitalului, psihologii și alți profesioniști au avut acces la datele pacienților prin profiluri false
- sistemul de management al poștelor personalului de specialitate s-a dovedit a fi deficitar, spitalul având 985 de profiluri medicale înregistrate în timp ce avea doar 296 de medici angajați.
- mai mult, profesioniști non-medicali (asistenți sociali) au avut acces la datele clinice ale pacienților prin intermediul acestui sistem

- potrivit art. 24 alin. (1) din cuprinsul Legii nr. 46/2003 privind drepturile pacienților, “pacientul are acces la datele medicale personale“
- potrivit art. 24 alin. (2) din cuprinsul Legii nr. 46/2003 privind drepturile pacienților, "pacientul are dreptul de a desemna, printr-un acord consemnat în anexa la foaia de observație clinică generală, o persoană care să aibă acces deplin, atât în timpul vieții pacientului, cât și după decesul pacientului, la informațiile cu caracter confidențial din foaia de observație“
- Legea nr. 46/2003 protejează printr-o serie de norme viața privată a pacientului
- potrivit art. 25 alin. (1) din cuprinsul Legii nr. 46/2003, "Orice amestec în viața privată, familială a pacientului este interzis, cu excepția cazurilor în care această imixtiune influențează pozitiv diagnosticul, tratamentul ori îngrijirile acordate și numai cu consimțământul pacientului“
- sunt considerate excepții cazurile în care pacientul reprezintă pericol pentru sine sau pentru sănătatea publică (art. 25 alin. (2) din cuprinsul Legii nr. 46/2003)
- o altă protecție importantă pe care GDPR o oferă persoanei vizate (pacientului) este desemnarea unui **responsabil de protecție a datelor**
- GDPR cere ca, în anumite cazuri, inclusiv atunci când datele sensibile sunt prelucrate pe scară largă, să fie desemnat un responsabil cu protecția datelor (DPO)
- instituțiile mari de asistență medicală, cum ar fi spitalul, trebuie să desemneze un DPO, având în vedere că procesează datele pacientului cu privire la starea sa de sănătate pe scară largă
- responsabilul cu protecția datelor are obligația de a respecta secretul sau confidențialitatea în ceea ce privește îndeplinirea sarcinilor sale
- responsabilul cu protecția datelor are obligația de a monitoriza respectarea prevederilor privind GDPR-ul

Responsabilul cu protecția datelor este desemnat pe baza calităților profesionale, și, în special, a cunoștințelor de specialitate în dreptul și practicile din domeniul protecției datelor, precum și pe baza capacității de a îndeplini sarcinile prevăzute de Regulament.

Responsabilul cu protecția datelor poate fi un membru al personalului operatorului sau poate să își îndeplinească sarcinile în baza unui contract de servicii.

Responsabilul cu protecția datelor are obligația de a respecta secretul sau confidențialitatea în ceea ce privește îndeplinirea sarcinilor sale, în conformitate cu dreptul Uniunii sau cu dreptul intern.

Sarcinile ( obligațiile) care îi incumbă responsabilului cu protecția datelor sunt prevăzute în cuprinsul art. 39 din Regulament.

***Obligațiile responsabilului cu protecția datelor:***

- ❖ ***informarea și consilierea*** operatorului, precum și a angajaților care se ocupă de prelucrare cu privire la obligațiile care le revin în temeiul prezentului Regulament și a altor dispoziții de drept intern referitoare la protecția datelor;
- ❖ ***monitorizarea*** respectării prezentului Regulament și a altor dispoziții de drept intern referitoare la protecția datelor;
- ❖ ***furnizarea de consiliere*** la cerere în ceea ce privește ***evaluarea impactului*** asupra protecției datelor și monitorizarea funcționării acesteia;
- ❖ ***cooperarea*** cu Autoritatea de Supraveghere.

Persoanele vizate ***pot contacta*** responsabilul cu protecția datelor cu privire la toate chestiunile legate de prelucrarea datelor lor și la exercitarea drepturilor lor în temeiul prezentului Regulament.

Operatorul și persoana împuternicită de operator ***sprijină*** responsabilul cu protecția datelor în îndeplinirea sarcinilor, asigurându-i resursele necesare pentru executarea acestor sarcini, precum și accesarea datelor cu caracter personal.

În situația în care personalul medical nu își îndeplinește obligațiile prevăzute în Regulamentul (UE) 2016/679, se poate aplica o sancțiune de către ANSPDCP (muștrare sau avertisment).

Personalul medical este obligat să respecte noul Regulament privind protecția datelor cu caracter personal. În cazul în care ANSPDCP constată lipsa conformității unei anumite acțiuni, va impune medicului să se conformeze și să adopte măsurile necesare pentru a evita o penalizare.