

**POLITICA DE SECURITATE
A PRELUCRĂRII DATELOR CU CARACTER PERSONAL ÎN
CADRUL IMSP SPITALUL CLINIC REPUBLICAN „TIMOFEI
MOȘNEAGA”**

Dispoziții generale

1. Prelucrarea datelor cu caracter personal constituie o procedură complexă, care implică o serie de măsuri tehnice și organizatorice având drept scop asigurarea protecției drepturilor fundamentale ale persoanelor fizice.

2. Politica de securitate a prelucrării datelor cu caracter personal (în continuare Politica) este elaborată în conformitate cu prevederile Legii nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal, cât și prevederile Hotărârii Guvernului nr. 1123 din 14.12.2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal.

3. Scopul politicii este de a asigura un nivel maxim de protecție a datelor cu caracter personal, prin aplicarea corespunzătoare a legislației naționale cu referire la protecția datelor, preîntâmpinarea scurgerii de informații, excluderea conexiunilor neautorizate și cuprinde un set de reglementări care determină modul de colectare, administrare, distribuire a datelor în cadrul IMSP Spitalul Clinic Republican „Timofei Moșneaga” (în continuare Spital).

4. Politica se aplică tuturor angajaților Spitalului, care sunt implicați direct sau indirect în procesul de colectare, prelucrare și păstrare a datelor cu caracter personal.

5. Responsabil de implementarea și monitorizarea respectării prevederilor Politicii de securitate a datelor cu caracter personal, este persoana desemnată prin ordinul directorului care va monitoriza respectarea prezentei politici și a altor acte normative referitoare la protecția datelor.

Principiile prelucrării datelor cu caracter personal

6. Prelucrarea datelor cu caracter personal în cadrul Spitalului se bazează pe următoarele principii:

a) legalitate, echitate și transparență – datele cu caracter personal sunt prelucrate cu bună-credință și în conformitate cu dispozițiile legale în vigoare, în mod echitabil și transparent față de persoana vizată;

b) limitarea scopului – datele cu caracter personal sunt colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri;

c) minimizarea datelor – datele cu caracter personal sunt adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate;

d) exactitate – datele cu caracter personal sunt exacte și, în cazul în care este necesar, să fie actualizate, se asigură că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere;

e) limitări legate de stocare – datele cu caracter personal nu trebuie păstrate decât în măsura necesară scopurilor pentru care sunt prelucrate; datele pot fi stocate pe perioade mai lungi în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, cu aplicarea măsurilor de ordin tehnic și organizatoric adecvate, în vederea garantării drepturilor și libertăților persoanei vizate;

f) integritate și confidențialitate – prelucrarea datelor personale trebuie făcută în condiții de siguranță, care să includă măsuri tehnice sau organizatorice corespunzătoare, care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale.

Temeiurile legale de prelucrare a datelor cu caracter personal

7. Datele cu caracter personal, prelucrate în cadrul Spitalului, sunt tratate în conformitate cu prevederile legislației în vigoare și normelor internaționale aplicabile, care reglementează protecția datelor cu caracter personal.

8. Executarea unui contract la care subiectul datelor cu caracter personal este parte a contractului.

9. În interesul legitim al Spitalului, cu condiția ca acest interes să nu prejudicieze interesele.

10. Consimțământul persoanei vizate (atunci când este cazul).

11. Înainte de încheierea unui contract (cu salariatul, pacientul, parteneri ș.a.), în timpul fazei de inițiere a contractului, datele cu caracter personal pot fi prelucrate pentru îndeplinirea solicitării.

Măsuri de protecție a datelor cu caracter personal

12. Măsurile de protecție a datelor cu caracter personal sunt asigurate în scopul:

a) preîntâmpinării scurgerii, modificării, copierii informației care conține date cu caracter personal prin metoda excluderii accesului neautorizat;

b) respectării cadrului normativ de operare a sistemelor informaționale și a programelor de prelucrare a datelor cu caracter personal;

c) asigurării caracterului complet, integru și veridic al datelor cu caracter personal în rețelele telecomunicaționale și resursele informaționale;

d) asigurării posibilității de gestionare a procesului de prelucrare și păstrare a datelor cu caracter personal;

e) preîntâmpinării conexiunilor neautorizate la rețelele telecomunicaționale și interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste rețele.

13. Pentru protecția datelor cu caracter personal este necesar a fi respectate un șir de acțiuni:

a) Folosirea metodelor de cifrare a acestei informații, precum și a canalelor VPN pentru a preîntâmpina scurgerea de informații care conțin date cu caracter personal, transmise prin canalele de legătură.

b) Folosirea mijloacelor de protecție speciale tehnice și de program, inclusiv a programelor licențiate, programelor antivirus, organizării sistemului de control al securității soft-ului și efectuarea periodică a copiilor de siguranță, pentru preîntâmpinarea distrugerii, modificării datelor cu caracter personal sau defecțiunilor în funcționarea soft-ului destinat prelucrării datelor cu caracter personal.

c) Efectuarea periodică a auditului intern al sistemelor informaționale.

d) Stabilirea exactă a ordinii de acces la informația care conține date cu caracter personal, prelucrate în cadrul sistemelor informaționale și de evidență instituite atât pentru utilizatorii interni cât și pentru cei externi.

e) În cazul neutilizării temporare a purtătorilor de informație pe suport de hârtie sau electronici care conțin date cu caracter personal, aceștia se păstrează în safeuri sau dulapuri metalice, care se încuie.

f) Computerele sau terminalele de acces și imprimantele sânt deconectate la terminarea sesiunilor de lucru.

g) Mijloacele de prelucrare, softurile destinate prelucrării datelor sunt scoase din perimetrul de Securitate doar în temeiul unei permisiuni scrise a conducerii.

h) Este interzisă instalarea programelor de tip Shareware și freeware fără aprobarea administratorului sistemului informatic.

i) Păstrarea confidențialității parolilor, interzicerea înscrierii acestora pe suport de hârtie.

j) Alegerea parolilor cu o mărime de minim 8 simboluri, care nu conțin simboluri identice consecutive și nu sunt compuse din aceleași litere sau cifre.

k) Dezactivarea procesului de salvare automată a parolilor.

l) Echipamentul electric utilizat pentru menținerea funcționalității sistemelor informaționale, cablurile electrice se va asigura contra deteriorărilor prin montarea lor în nișe speciale.

m) În cazul apariției situațiilor de avarie sau de forță majoră se va asigura posibilitatea deconectării electricității de la sistemele informaționale.

n) Accesul fără fir la sistemele informaționale de date cu caracter personal este limitat la maximum, este documentat, supus monitorizării și controlului.

o) Este asigurată protecția contra infiltrării programelor dăunătoare în softurile destinate prelucrării datelor cu caracter personal, prin existența programelor anti-virus.

p) În cazul în care, raporturile de muncă ale salariatului Spitalului au încetat, au fost suspendate, absența salariatului la postul de muncă pe parcursul unei perioade îndelungate (mai mult de 2 luni), sau conform noile atribuții de funcție nu necesită

accesul la datele cu caracter personal, accesul utilizatorului la sistem se revocă sau se suspendă.

Drepturile subiecților datelor cu caracter personal

14. Subiecții datelor cu caracter personal au următoarele drepturi:

a) Să obțină în mod gratuit informațiile privind datele sale cu caracter personal prelucrate în cadrul Spitalului, scopul prelucrării, categoriile de date, destinatarii cărora le sunt dezvăluite aceste date etc.

b) Să dispună de acces liber la datele sale cu caracter personal.

c) Să intervină asupra datelor cu caracter personal prin: rectificarea, actualizarea, blocarea sau ștergerea datelor cu caracter personal a căror prelucrare contravine legii.

d) Să se adreseze organului de control al prelucrărilor de date cu caracter personal în cazul încălcării legislației în vigoare ce vizează protecția datelor cu caracter personal.

e) De a retrage în orice moment consimțământul exprimat anterior privind prelucrarea datelor cu caracter personal, fără a afecta legalitatea prelucrărilor efectuate înainte de retragerea acestuia.

Categorii de date cu caracter personal prelucrate

15. În dependență de scopul prelucrării datelor cu caracter personal și/sau derularea relației contractuale cu Spitalul (salariat, pacient, partener), dar și având în vedere specificul activităților desfășurate, pot fi prelucrate următoarele categorii de date cu caracter personal:

a) date generale de identificare: nume, prenume, patronimic și pseudonim (după caz), data și locul nașterii, cetățenia;

b) date de contact: domiciliul și reședința (dacă este cazul), numărul de telefon/fax, adresa de poștă electronică;

c) date atribuite de autorități publice: codul numeric personal, seria și numărul actului de identitate;

d) semnătura electronică, semnătura olografă;

e) date privind starea de sănătate;

f) date biometrice sau de recunoaștere facială utilizarea unui sistem de identificare a angajaților prin mijloace electronice, care contrapune poza preluată din Registrul de stat al populației;

g) date bancare: coduri de identificare, coduri IBAN atașate conturilor bancare, numerele cardurilor de plată, data expirării cardurilor, precum și alte date de identificare a cardurilor bancare;

h) imagini: foto din actul de identitate furnizat și video înregistrată de camere de supraveghere video instalate în sediile Spitalului;

i) date privind studiile, formarea profesională, locuri de muncă anterioare;

16. Spitalul evită să prelucreze date din categoria specială a datelor cu caracter personal:

- a) originea rasială sau etnică, convingerile politice, religioase, cele privind condamnările penale, cu excepția cazurilor prevăzute de lege;
- b) date privind situația familială: starea civilă, persoane aflate la întreținere;
- c) date privind situația financiară: venituri, tranzacții bancare și istoricul acestora, bunurile deținute în proprietate;
- d) apartenența politică: informații legate de calitatea de persoană expusă politic, în cazurile specifice, care sunt prelucrate doar în cazurile prevăzute de legislația privind prevenirea și combaterea spălării banilor și finanțării terorismului;
- e) convingerile politice și religioase ale salariatului, precum și la viața privată a acestuia. În cazurile prevăzute de lege, angajatorul poate cere și prelucra date despre viața privată a salariatului numai cu acordul scris al acestuia;
- f) alte date cu caracter personal care nu au relevanță cu scopul prelucrării.

Prelucrarea datelor cu caracter personal

17. Prelucrarea datelor cu caracter personal înseamnă orice operațiune sau serie de operațiuni care se efectuează asupra datelor cu caracter personal prin mijloace automatizate sau neautomatizate, cum ar fi colectarea, înregistrarea, organizarea, stocarea, păstrarea, restabilirea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvoltarea prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ștergerea sau distrugerea, indiferent dacă sunt efectuate prin mijloace automate sau neautomatizate.

18. Consimțământul pacientului privind prelucrarea datelor cu caracter personal nu este necesar a fi întocmit în formă scrisă având în vedere excepția prevăzută de art. 5 alin. (5) lit.b), c), d) din Legea nr. 133 din 08.07.2011, potrivit căruia pot fi prelucrate date privind starea de sănătate atunci, când prelucrarea este necesară din motive de interes public major sau pe motivul protejării vieții, sănătății subiectului datelor cu caracter personal sau îndeplinirii unei obligații care îi revine operatorului/instituției medicale conform legii.

19. Colectarea și prelucrarea datelor cu caracter personal privind starea de sănătate trebuie să fie efectuate numai de către cadrele medicale sau de persoane sau entități, care acționează în numele acestor specialiști. Operatorii, care nu sunt specialiști în domeniul sănătății, dar sunt împuterniciți cu asemenea atribuții trebuie să colecteze și să prelucreze date cu caracter personal doar cu respectarea regulilor de confidențialitate echivalente cu cele ce revin unui cadru medical.

20. Prelucrarea datelor cu caracter personal în cadrul sistemelor informaționale automatizate se face de către persoana căreia i s-a atribuit un identificator în vederea utilizării Sistemului Informațional Automatizat „Asistența Medicală Spitalicească (SIA AMS). Scopul prelucrării este doar pentru identificarea pacientului și acordarea asistenței medicale acestuia. Se interzice transmiterea datelor de utilizator și a parolei către alte persoane. Pentru încălcarea acestei obligații personalul medical va purta răspundere civilă, contravențională etc.

21. Informația privind starea de sănătate, rezultatele investigațiilor, diagnosticul, pronosticul, tratamentul sunt date confidențiale și urmează a fi protejate de către personalul medico-sanitar. Prelucrarea datelor cu caracter personal

privind starea de sănătate a unei persoane reprezintă o prelucrare sensibilă, aptă să genereze riscuri considerabile în adresa drepturilor subiecților de date. Toate datele conținute în documentația medicală, în dosarul pacientului și în sistemele informaționale ce prelucrează și sunt „confidențiale”.

22. Toate cadrele medicale, care au acces la date cu caracter personal urmează a fi supuse unei clauze de confidențialitate, care va fi inclusă în contractul de muncă sau/și în fișa postului cu mențiunea despre posibilitatea atragerii la răspundere civilă, contravențională ori penală pentru încălcarea acesteia.

23. În scopul asigurării drepturilor și libertăților omului și cetățeanului, în procesul prelucrării datelor personale ale salariatului, angajatorul va prelucra datele personale ale salariatului, exclusiv în scopul acordării de asistență la angajare, instruirii și avansării în serviciu, asigurării securității personale a salariatului, controlului volumului și calității lucrului îndeplinit și asigurării integrității bunurilor unității;

Securitatea mediului fizic și a tehnologiilor informaționale folosite în procesul prelucrării datelor cu caracter personal

24. Accesul în sediile/oficiile/birourile ori spațiile unde sunt amplasate sistemele informaționale de date cu caracter personal este interzis, cu excepția persoanelor care dispun de autorizația necesară, conform listei sau însemnelor corespunzătoare (insigne, ecusoane, cartele de identificare).

25. Se asigură administrarea și monitorizarea accesului fizic în toate punctele de acces la sistemele informaționale de date cu caracter personal, inclusiv se reacționează la încălcarea regimului de acces.

26. Perimetrul de securitate reprezintă perimetrul oficiilor, în care se prelucrează/stochează date cu caracter personal.

27. Perimetrul clădirii sau încăperilor în care sunt amplasate mijloacele de prelucrare a datelor cu caracter personal este integru din punct de vedere fizic. Pereții exteriori ai încăperilor sunt rezistenți, intrările sunt echipate cu lacăte și semnalizare.

28. Amplasarea mijloacelor de prelucrare a datelor cu caracter personal corespunde necesităților asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri.

29. Ușile și ferestrele se încuie în cazul în care în încăpere nu este nimeni. Computerele, serverele și alte terminale de acces sunt amplasate în locuri cu acces limitat pentru persoane străine. Accesul în perimetrul de securitate a clădirii, unde se prelucrează/stochează date cu caracter personal cu utilaje foto/video neautorizate este interzis, ținând cont de necesitatea asigurării regimului de confidențialitate și securitate a prelucrării datelor cu caracter personal. Folosirea tehnicii foto, video, audio sau altor mijloace de înregistrare în perimetrul de securitate este admisă doar în cazul prezenței permisiunii speciale a conducerii.

30. Imaginile video prelucrate prin intermediul mijloacelor de supraveghere video vor fi stocate pe o perioadă de maxim 90 de zile. Spitalul poate păstra înregistrările video pe un termen extins, având ca temei interesul legitim, și anume: apărarea drepturilor și intereselor spitalului/subiectului datelor cu caracter personal

în instanța de judecată, interacțiunea cu autoritățile publice, demararea anchetelor/investigațiilor interne.etc

Stocarea și accesul la datele cu caracter personal

31. Datele cu caracter personal vor fi stocate pe o perioadă strict prevăzută de actele normative. Instituția medicală păstrează acte ce conțin date cu caracter personal în baza Ordinului nr. 158 din 01 octombrie 2024 „Cu privire la punerea în aplicare a Nomenclatorului dosarelor IMSP SCR „Timofei Moșneaga”.

Persoana responsabilă de prelucrarea datelor cu caracter personal

32. Persoana responsabilă cu protecția datelor desemnată prin Ordinul nr. 131 din 11.08.2022, va exercita următoarele sarcini:

a) informarea și consilierea operatorului sau a persoanei împuternicite de operator, precum și a angajaților care se ocupă de prelucrarea datelor cu privire la obligațiile care le revin în temeiul prezentei politici și al altor acte normative;

b) monitorizarea respectării prezentei politici și a altor acte normative referitoare la protecția datelor și a politicilor operatorului sau ale persoanei împuternicite de operator în ceea ce privește protecția datelor cu caracter personal, precum și atribuirea responsabilităților, inclusiv privind acțiunile de sensibilizare și de formare a personalului implicat în operațiunile de prelucrare și privind auditurile aferente;

c) oferirea consilierii la cerere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia;

d) cooperarea cu Centrul pentru Protecția datelor cu Caracter personal;

e) asumarea rolului de punct de contact pentru subiecții implicați în prelucrarea datelor în cadrul Spitalului.

Controlul intern privind respectarea datelor cu caracter personal cât și raportarea incidentelor de securitate va fi efectuat respectându-se ierarhia funcțiilor: angajați - șefi de secții/servicii; șefi de departamente - administrația spitalului.

Incidentele asupra DCP vor fi colectate de către persoana desemnată responsabilă de protecția datelor în instituție. Oricine poate raporta direct incidentele privind protecția datelor direct persoanei desemnate responsabile de protecția datelor în instituție. Raportarea incidentelor se va face verbal sau scris la adresa de email datepersonale@scr.md.

Controlul extern al legalității prelucrării datelor se efectuează de către Centru Național pentru Protecția Datelor cu Caracter Personal (Centru).