MINISTERUL SĂNĂTĂȚII AL REPUBLICII MOLDOVA
Instituția Medico-Sanitară Publică
SPITALUL CLINIC REPUBLICAN „Timofei Moșneaga”

ORDIN

"06" martie 2026 Nr. 44

Cu privire la aprobarea „Politicii de confidențialitate a datelor cu caracter personal în cadrul IMSP Spitalul Clinic Republican „Timofei Moșneaga”

În conformitate cu Legea nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal, 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, având în vedere necesitatea asigurării unui nivel adecvat de securitate a datelor cu caracter personal, în scopul stabilirii măsurilor organizatorice și tehnice necesare prelucrării legale, sigure și transparente a acestora, precum și în temeiul Regulamentului de organizare și funcționare a IMSP Spitalul Clinic Republican „Timofei Moșneaga” aprobat prin Ordinul Ministerului Sănătății nr.404 din 05.05.2023,

ORDON:

1. Se aprobă „Politica de confidențialitate a datelor cu caracter personal în cadrul IMSP Spitalul Clinic Republican „Timofei Moșneaga”, conform anexei la pezentul ordin.
2. Șefii de departamente și secții se desemnează responsabili pentru aducerea la cunoștința personalului din subordine și monitorizarea respectării prevederilor politicii aprobate.
3. Serviciul informațional și telecomunicații se desemnează responsabil pentru:
- aplicarea măsurilor tehnice de protecție a tehnologiei informației și comunicațiilor;
- asigurarea integrității informației care conține date cu caracter personal;
- administrarea accesului, precum și soluții practice de reacționare la eventuale incidente de securitate.
4. Secția comunicare și secretariat va aduce la cunoștința tuturor șefilor de subdiviziuni prevederile prezentului ordin, sub semnătură.
5. Se abrogă Ordinul nr. 17 din 26 ianuarie 2026 „Cu privire la aprobarea „Politicii de securitate a prelucrării datelor cu caracter personal".
6. Controlul executării prezentului ordin mi-l asum.

Director interimar **Andrei UNCUȚA**

Anexă
la ordinul nr. 44 din 06.03.2026

POLITICA DE CONFIDENȚIALITATE
a datelor cu caracter personal în cadrul IMSP Spitalul Clinic Republican „Timofei Moșneaga”

I. Dispoziții introductive

1.1. Prezenta Politică determină securitatea datelor cu caracter personal în cadrul IMSP Spitalul Clinic Republican „Timofei Moșneaga” (în continuare - IMSP SCR „Timofei Moșneaga”), cadrul necesar de aplicare a Convenției de la Strasburg din 28.01.1981 pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal și cerințele față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale.

1.2. Cerințele față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal au drept scop stabilirea regulilor minime de implementare de către deținătorii de date cu caracter personal a măsurilor tehnice și organizatorice necesare pentru asigurarea securității, confidențialității și integrității datelor cu caracter personal prelucrate în cadrul sistemelor informaționale de date cu caracter personal și/sau registrelor ținute manual, in conformitate cu prevederile Legii nr.133/2011 privind protecția datelor cu caracter personal și altor acte normative ale Ministerului Sănătății, ce vizează protecția datelor cu caracter personal și confidențiale.

1.3. Sunt supuse protecției toate resursele informaționale ale deținătorilor de date cu caracter personal, care conțin date cu caracter personal.

1.4. Protecția datelor cu caracter personal în sistemele informaționale de date cu caracter personal este asigurată în **scopul**:

a) preîntâmpinării scurgerii informației care conține date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta;

b) preîntâmpinării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal;

c) respectării cadrului normativ de folosire a sistemelor informaționale vizând prelucrarea datelor cu caracter personal;

d) asigurării caracterului complet, integru, veridic al datelor cu caracter personal în resursele informaționale;

e) păstrării posibilităților de gestionare a procesului de prelucrare și păstrare a datelor cu caracter personal;

f) preîntâmpinării acțiunilor intenționate și/sau neintenționate a utilizatorilor interni și/sau externi, precum și a altor angajați ai deținătorului de date cu caracter personal, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program.

II. Noțiunile principale:

autentificare – verificarea identificatorului atribuit subiectului de acces, confirmarea autenticității;

categorii speciale de date cu caracter personal – datele care dezvăluie originea rasială sau etnică a persoanei, convingerile ei politice, religioase sau filozofice, apartenența socială, datele privind starea de sănătate sau viața sexuală, precum și cele referitoare la condamnările penale, măsurile procesuale de constrângere sau sancțiunile contravenționale;

consimțământul subiectului de date cu caracter personal – manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a subiectului de date prin care acesta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care îl privesc să fie prelucrate;

date cu caracter personal - date despre o persoană fizică, ce permit identificarea ei directă sau indirectă;

subiect al datelor cu caracter personal - persoană fizică, purtătoare de date cu caracter personal;

prelucrarea datelor cu caracter personal - orice operațiune sau set de operațiuni care se efectuează asupra datelor cu caracter personal la colectare, înregistrare, organizare, stocare, precizare, adaptare, modificare, excludere, consultare, acordare a accesului, utilizare, transmitere, difuzare, blocare sau distrugere;

transmiterea datelor cu caracter personal - punerea la dispoziția terților a datelor cu caracter personal de către deținătorul acestora;

nivel de protecție – nivel de securitate proporțional riscului pe care îl comportă prelucrarea față de datele cu caracter personal respective, precum și față de drepturile și libertățile persoanelor, stabilit conform Cerințelor, elaborat și actualizat corespunzător nivelului dezvoltării tehnologice și costurilor implementării acestor măsuri;

persoana responsabilă de politica de securitate a datelor cu caracter personal – persoana responsabilă de funcționarea corespunzătoare a sistemului complex de protecție a informației care conține date cu caracter personal, precum și de elaborarea, implementarea și monitorizarea respectării prevederilor politicii de securitate a deținătorului de date cu caracter personal;

protecția informației contra acțiunilor neintenționate – ansamblu de măsuri orientate spre prevenirea acțiunilor neintenționate, provocate de erorile utilizatorului, defectele mijloacelor tehnico-aplicative, fenomenele naturii sau alte cauze ce nu au ca scop direct modificarea informației, dar care conduc la distorsiunea, distrugerea, copierea, blocarea accesului la informație, precum și la pierderea, distrugerea acesteia sau la defectarea suportului material al informației care conține date cu caracter personal;

purtător de date cu caracter personal – suport magnetic, optic, laser, de hârtie sau alt suport al informației pe care se creează, se fixează, se transmite, se recepționează, se păstrează sau, în alt mod, se utilizează documentul și care permite reproducerea acestuia;

sistem informațional de date cu caracter personal – totalitatea resurselor și tehnologiilor informaționale interdependente, de metode și de personal, destinată păstrării, prelucrării și furnizării de informație care conține date cu caracter personal;

tehnologie informațională (TI) – totalitatea metodelor, procedeelor și mijloacelor de prelucrare și transmitere a informației care conține date cu caracter personal și regulile de aplicare a acesteia;

stocare – păstrarea pe orice fel de suport a datelor cu caracter personal;

utilizator – persoana care acționează sub autoritatea deținătorului de date cu caracter personal, cu drept recunoscut de acces la sistemele informaționale de date cu caracter personal;

III. Aspecte generale

3.1. Politica reprezintă actul normativ departamental, cu forță juridică obligatorie, respectarea căreia este asigurată de prevederile actelor normative din domeniul protecției datelor cu caracter personal și este documentul ierarhic superior în nomenclatorul actelor interne cu privire la prelucrarea datelor cu caracter personal;

3.2. Politica aplică soluții practice cu un nivel de detaliere și complexitate proporțional, în partea ce ține de identificarea și autentificarea utilizatorilor; de reacționare la incidentele de securitate; de protecție a tehnologiilor informaționale și comunicațiilor; de asigurare a integrității informației care conține date cu caracter personal; de administrare a accesului; de audit și asigurare a evidenței, luând în considerare:

- categoriile datelor cu caracter personal;
- operațiunile de prelucrare efectuate datelor cu caracter personal;
- dimensiunea IMSP SCR „Timofei Moșneaga" în funcție de numărul angajaților, numărul subdiviziunilor administrative etc;
- formele de ținere a registrelor în care sunt prelucrate date cu caracter personal (manuală, electronică sau mixtă);
- complexitatea sistemelor informaționale de date cu caracter personal și programelor de aplicații implicate în procesul de prelucrare a datelor;
- riscurile la care este expusă IMSP SCR „Timofei Moșneaga" sau persoanele ale căror date cu caracter personal sunt prelucrate, starea de dezvoltare tehnologică în acest domeniu și costul măsurilor de implementare.

3.3. Politica se multiplică și se aduce la cunoștința angajaților IMSP SCR „Timofei Moșneaga", în limitele competențelor funcționale și nivelului de acces acordat la date cu caracter personal.

3.4. Semnarea în fișa de evidență a multiplicării Politicii confirmă aducerea la cunoștință a Politicii și presupune asumarea responsabilității de către persoana vizată (fizică sau juridică) a Cerințelor care necesită a fi asigurate la prelucrarea datelor cu caracter personal.

IV. Cadrul juridic aplicabil

4.1. La prelucrarea datelor cu caracter personal sunt respectate următoarele acte:

La nivel internațional/european:

- Convenția nr.108 pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal;
- Practica Curții Europene a Drepturilor Omului;
- Recomandările Consiliului de Miniștri, Autorității Europene de Protecție a Datelor și Comitetului european pentru protecția datelor (CEPD);
- Regulamentul General privind Protecția Datelor nr. 679/2016 (GDPR).

Cadrul juridic național:
- Constituția Republicii Moldova;
- Codul muncii al Republicii Moldova, nr.154/2003;
- Legea nr. 263/2005 cu privire la drepturile și responsabilitățile pacientului;
- Legea nr. 264/2005 cu privire la exercitarea profesiunii de medic;
- Legea nr. 23/2007 cu privire la profilaxia infecției HIV/SIDA;
- Legea nr. 10/2009 privind supravegherea de stat a sănătății publice;
- Legea nr. 411/1995 ocrotirii sănătății;
- Legea nr. 338/1994 privind drepturile copiilor;
- Legea nr. 1402/1997 privind sănătatea mentală;
- Legea nr. 133/2011 privind protecția datelor cu caracter personal;
- Legea nr. 105/2003 privind protecția consumatorului;
- Legea nr.71/2007 cu privire la registre;
- Legea nr.467/2003 cu privire la informatizare și resursele informaționale de stat;
- Legea nr. 284/2004 privind serviciile societății informaționale ;
- Legea nr. 1069/2000 cu privire la informatică.

V. Principiile generale de conformitate la prelucrarea datelor

5.1. Datele cu caracter personal care fac obiectul unei prelucrări, trebuie să fie prelucrate:

- corect și conform prevederilor legale - orice colectare și ulterior prelucrare de date cu caracter personal urmează să se facă în strictă conformitate cu procedura și cu necesitatea ce rezultă expres din prevederile actelor normative. Aceasta presupune, că înainte de a colecta, utiliza și dezvălui datele cu caracter personal, acest fapt trebuie să rezulte expres dintr-un drept sau obligație legală;
- în scopuri determinate, explicite și legitime, iar ulterior să nu fie prelucrate într-un scop incompatibil - înainte de a fi colectate și utilizate datele cu caracter personal, acestea urmează a fi raportate exhaustiv la scopul în care sunt colectate acestea, cu stabilirea concretă a sistemului de evidență a datelor cu caracter personal în care se vor prelucra astfel de date, norma legală care oferă un atare drept. Datele colectate într-un scop nu pot fi utilizate în oricare alt scop, decât cu consimțământul subiectului de date, dacă legea nu prevede altfel;

- adecvat, pertinent și neexcesiv - atât la colectarea datelor cu caracter personal cât și la stocarea, utilizarea sau prelucrarea în orice alt fel se va efectua raportarea volumului categoriilor de date cu caracter personal prelucrate la necesitatea reală a IMSP SCR „Timofei Moșneaga". În acest sens, se va ține cont de principiul minimizării datelor cu caracter personal colectate și verificării periodice sau la necesitate asupra pertinenței și caracterului neexcesiv al datelor prelucrate;

- exact și actualizat - IMSP SCR „Timofei Moșneaga" va colecta datele cu caracter personal din actele de identitate, de la subiectul de date, din sistemele informațional de stat și private, sau alte surse veridice. Actualizarea datelor cu caracter personal se va efectua sistematic.

- pe o perioadă care nu va depăși durata necesară atingerii scopurilor pentru care sunt colectate și ulterior prelucrate, datele cu caracter personal se vor stoca doar până la atingerea scopului pentru care datele au fost colectate, conducându-se de legislația în vigoare.

5.2. În cazul, în care informația cu accesibilitate limitată este utilizată de către angajatul IMSP SCR „Timofei Moșneaga" în alte scopuri, decât cele prestabilite expres de IMSP SCR „Timofei Moșneaga", aceste activități se consideră a fi contrare acestor reglementări. În acest sens, angajatul se va constitui în calitate de operator de date distinct de IMSP SCR „Timofei Moșneaga", responsabilitatea juridică și răspunderea prevăzută de legislația în vigoare se aplică exclusiv în privința acestuia.

5.3. Persoanele implicate în procesul de prelucrare a datelor cu caracter personal, terțe persoane, în vederea îndeplinirii de către acestea a atribuțiilor funcționale și asumării responsabilităților de securitate a datelor cu caracter personal, inclusiv asupra confidențialității acestora, definesc clar responsabilitățile și procesele de securitate a datelor cu caracter personal, asigură măsuri tehnice și organizaționale necesare organizării procesului de securitate a datelor cu caracter personal.

VI. Categoriile de date cu caracter personal

6.1. Datele cu caracter personal, care direct sau indirect identifică o persoană fizică, în special, prin referire la un număr de identificare (cod personal), la unul sau mai multe elemente specifice proprii identității sale fizice, fiziologice, psihice, economice, culturale sau sociale, se împart in două categorii: obișnuite și speciale.

6.2. Categoria datelor obișnuite o constituie informația referitoare la persoane fizice identificate, care sunt înregistrate în instituție și beneficiază de asistență medicală, **referitoare la salariații instituției și care dezvăluie**:

- numele și prenumele;
- sexul;
- data și locul nașterii;
- cetățenia;
- IDNP;
- poza;

- situația familială;
- situația militară;
- datele bancare;
- semnătura;
- CPAS;
- datele personale ale membrilor de familie;
- numărul de telefon, mobil;
- adresa de domiciliu;
- adresa e-mail;
- profesia și/sau locul de muncă;
- formarea profesională, diploma, studii.

6.3. Categoria datelor speciale a datelor cu caracter personal o constituie informația privind starea de sănătate sau viața intimă a persoanelor ce sunt înregistrate și au apelat la asistență medicală, măsuri profilactice, etc.

VII. Prelucrarea datelor cu caracter personal

7.1. Prelucrarea datelor cu caracter personal se efectuează cu consimțământul necondiționat al pacientului, cu excepția cazurilor prevăzute de cadrul normativ.

7.2. În cazul incapacității subiectului datelor cu caracter personal, consimțământul la prelucrarea datelor lui cu caracter personal se acordă în formă scrisă de către reprezentantul legal al subiectului datelor cu caracter personal.

7.3. În cazul decesului subiectului datelor cu caracter personal, consimțământul la prelucrarea datelor lui cu caracter personal se acordă, în formă scrisă, de către succesorii subiectului datelor cu caracter personal, dacă un astfel de consimțământ nu a fost dat de subiectului datelor cu caracter personal în timpul vieții.

7.4. Obținerea consimțământului va fi la prima adresare în cadrul IMSP SCR „Timofei Moșneaga", cu atașarea pe prima filă a fișei medicale de ambulatoriu sau a bolnavului de staționar. Ulterior la fiecare adresare, până la acordarea asistenței medicale, se verifică existența consimțământului.

7.5. Refuzul pacientului de a-și exprima consimțământul pentru prelucrarea datelor personale face imposibilă acordarea serviciilor medicale (cu excepția urgențelor majore).

7.6. Familiarizarea beneficiarilor de servicii, inclusiv părinților copiilor, referitor la scopul și efectele consimțământului se efectuează de către asistentele medicale ale medicilor de familie și specialiști, medicii de familie și medicii specialiști.

7.7. Șefii de secții, managerii, vicedirectorii reieșind din specificul activității, organizează măsurile de securitate a datelor cu caracter personal, inclusiv procedurile și măsurile legate de realizarea acestei proceduri cu aplicarea soluțiilor practice.

7.8. Salariații instituției sunt instruiți referitor la cunoașterea categoriilor de date cu caracter personal supuse prelucrării, cerințele de protecție a acestora, precum și principiile operațiunilor de prelucrare efectuate asupra lor. Responsabili

de instruire sunt șefii de subdiviziuni (la angajare-instruire primară), iar vicedirectorii periodic la necesitate.

7.9. Salariații efectuează prelucrarea datelor cu caracter personal conform atribuțiilor funcționale. Nu se admite prelucrarea datelor cu caracter personal în alte scopuri, decât în scopul exercitării obligațiunilor funcționale.

7.10. Directorul IMSP SCR „Timofei Moșneaga" numește vicedirectorii, șefii de subdiviziuni și șeful Serviciului tehnologii informaționale ca persoane responsabile de elaborarea, implementarea și monitorizarea respectării prevederilor Politicii de securitate a datelor cu caracter personal.

7.11. Șefii secțiilor, subdiviziunilor, asistentele superioare poartă responsabilitate pentru organizarea și controlul măsurilor contra divulgării, prelucrării neautorizate, distrugerii, denaturării, furtului, pierderii actelor medicale sau încălcarea confidențialității datelor cu caracter personal.

7.12. Este interzisă transmiterea fișelor medicale, în original, pacienților în mod neautorizat.

7.13. Nu se admite divulgarea datelor cu caracter personal persoanelor terțe, prin telefon sau prin comunicare directă fără stabilirea identității persoanei și a temeiului legal al solicitării.

7.14. Nu se admite divulgarea datelor cu caracter personal în discuții dintre salariați cu excepția cazurilor de necesitate de serviciu.

7.15. Angajații IMSP SCR „Timofei Moșneaga" sunt obligați să explice pacienților, solicitanților motivele nedivulgării datelor cu caracter personal sau refuzul eliberării extraselor, fișelor, certificatelor, etc.

7.16. Utilizatorii datelor cu caracter personal din IMSP SCR „Timofei Moșneaga" vor semna un angajament de confidențialitate (nedivulgare neautorizată a datelor cu caracter personal și medical).

VIII. Asigurarea securității datelor cu caracter personal la prelucrarea manuală

8.1. Măsurile de protecție a datelor cu caracter personal vor fi efectuate permanent de către toți colaboratorii medicali și personal auxiliar din cadrul IMSP SCR „Timofei Moșneaga", implicați în acordarea asistenței medicale (registratori, asistente medicale, medici, medici rezidenți, șefi de secție, secretariat, arhivă, personal administrativ) deținători de date cu caracter personal.

8.2. Este interzisă prelucrarea și transmiterea ilicită a datelor cu caracter personal. Asigurarea confidențialității, confirmată prin semnătura utilizatorilor datelor cu caracter personal și medical, preîntâmpinarea de răspundere în cazul divulgării necondiționate.

8.3. În lipsa adoptării măsurilor de protecție este interzisă realizarea lucrărilor cu prelucrarea datelor cu caracter personal.

8.4. Protecției este supusă documentația medicală primară - note informative la cazuri de deces, recenzii, certificate, extrase, trimiteri la investigații etc.

8.5. Metodele de protecție a datelor cu caracter personal sunt:

- excluderea accesului neautorizat la datele cu caracter personal;

- preîntâmpinarea acțiunilor intenționate și/sau neintenționate, care ar condiționa modificarea sau distrugerea datelor cu caracter personal;

- acces la informație determinat strict de exercitarea obligațiunilor funcționale.

VIII. Responsabilități și obligațiuni

8.1. Principala responsabilitate în elaborarea, implementarea și monitorizarea aplicării prevederilor Politicii revine persoanei responsabile cu protecția datelor cu caracter personal (în continuare Persoana responsabilă cu protecția datelor).

8.2. IMSP SCR „Timofei Moșneaga" a decis asupra necesității desemnării unui angajat în calitate de persoană responsabilă cu protecția datelor cu caracter personal, în conformitate cu art.25 din Legea nr.133/2011 privind protecția datelor cu caracter personal.

8.3. Persoana responsabilă cu protecția datelor, indiferent de funcțiile exercitate, în cadrul monitorizării implementării/respectării prevederilor Politicii se subordonează nemijlocit directorului IMSP SCR „Timofei Moșneaga" sau persoanei care îndeplinește interimatul funcției.

8.4. Persoana responsabilă cu protecția datelor nu poate fi supusă sau subordonată nici unei indicații sau cerințe indiferent de către cine a fost înaintată, în cazul în care această solicitare în mod vădit produce coliziune cu regimul juridic al protecției datelor cu caracter personal.

8.5. Obligațiile IMSP SCR „Timofei Moșneaga" în raport cu Persoana responsabilă cu protecția datelor:

- de a implica Persoana responsabilă cu protecția datelor în mod corespunzător și în timp util în toate aspectele legate de protecția datelor cu caracter personal. Aceste aspecte se referă la modul de prelucrare a datelor și a mijloacelor utilizate în acest sens, transferul transfrontalier și măsurile de conformitate și securitate la prelucrarea datelor cu caracter personal;

- de a oferi suport și de a sprijini Persoana responsabilă cu protecția datelor în îndeplinirea sarcinilor sale, asigurându-i resursele necesare administrative (timp, resurse umane, echipament, soft) și financiare, pentru executarea acestor atribuții;

- de a oferi acces liber la informația necesară pentru îndeplinirea funcțiilor sale, în măsura în care acesta nu operează în afara cadrului Politicii;

- de a oferi accesul la locațiile unde sunt prelucrate datele, inclusiv la datele personale, la regulamente, instrucțiuni, ordine, dispoziții ce se referă la protecția datelor cu caracter personal;

- de a nu sancționa, demite sau restrânge Persoana responsabilă cu protecția datelor prin anumite măsuri administrative pentru îndeplinirea sarcinilor sale în corespundere cu cadrul normativ;

- de a informa Persoana responsabilă cu protecția datelor, că poartă răspundere în conformitate cu legislația civilă, contravențională și/sau penală, pentru exercitarea cu rea credință a sarcinilor și împuternicirilor de care dispune;

- de a informa Persoana responsabilă cu protecția datelor să nu primească indicații sau instrucțiuni care ar putea duce la încălcarea regimului juridic de protecție a datelor cu caracter personal;

- de a informa Persoana responsabilă cu protecția datelor să nu primească indicații sau instrucțiuni care ar putea genera un conflict de interese;

- de a comunica Persoanei responsabile cu protecția datelor că este autorizat să efectueze măsuri de instruire, simulare și control a implementării și respectării Politicii în cadrul IMSP SCR „Timofei Moșneaga";

- de a delega, în caz de necesitate, o parte din responsabilitățile funcționale prevăzute de Politică către alți angajați printr-un ordin corespunzător.

8.6. Sarcinile, obligațiile și responsabilitățile Persoanei responsabile cu protecția datelor:

- informează și oferă consiliere IMSP SCR „Timofei Moșneaga" și/sau persoanelor împuternicite de către IMSP SCR „Timofei Moșneaga", precum și angajaților în activități legate de prelucrarea datelor cu caracter personal, respectarea Politicii, cadrul legal din domeniul protecției datelor cu caracter personal;

- informează și explică drepturile subiecților de date cu caracter personal;

- oferă suport la examinarea cererilor, plângerilor, sesizărilor, reclamațiilor înaintate în contextul domeniului protecției datelor cu caracter personal;

- monitorizează respectarea prezentei Politici și a cerințelor din domeniul protecției datelor cu caracter personal;

- oferă suport și consiliere la evaluarea impactului asupra protecției datelor cu caracter personal;

- reprezintă operatorul pe problemele legate de domeniul protecției datelor cu caracter personal;

- informează operatorul, persoanele împuternicite de către operator și angajații acestora despre tendințele și modificările în domeniul protecției datelor cu caracter personal;

- cooperează cu Autoritatea de supraveghere, inclusiv ca punct de contact în cazul consultării prealabile cu aceasta;

- asigură confidențialitatea și nedivulgarea informațiilor cu care a făcut cunoștință în cadrul realizării sarcinilor și activităților în calitate de responsabil cu protecția datelor cu caracter personal;

- dispune de cunoștințe de specialitate în dreptul și practicile din domeniul protecției datelor cu caracter personal și le perfectează sistematic în corespundere cu tendințele din domeniul protecției datelor;

- efectuează instruirea noilor angajați privind principiile de protecție a datelor cu caracter personal;

- efectuează instruirea angajaților privitor la principiile de protecție a datelor cu caracter personal;

- menține registrul de evidență a persoanelor instruite;

- stabilește orarul controalelor de securitate, în conformitate cu regulamentul de securitate al fiecărui Sistem de date cu caracter personal. Controalele de securitate se realizează sistematic (o dată în an/jumătate de an).

Prin intermediul acestor controale se face o evaluare suplimentară prin care se vede dacă se respectă cerinţele de protecţie a datelor, de către persoanele responsabile de aceste sisteme;

- menţine registrul controalelor de securitate;
- înregistrează rapoartele despre incidentele de securitate în registrul de evidenţă;
- este responsabil de aducerea la cunoştinţa angajaţilor IMSP SCR „Timofei Moşneaga" a Politicii, eliberarea copiilor şi modificarea ei.

IX. Drepturile subiecţilor de date cu caracter personal

9.1. Dreptul la informare, constă în dreptul de a fi informat cu privire la identitatea IMSP SCR „Timofei Moşneaga", scopul în care se face prelucrarea datelor, destinatarii sau categoriile de destinatari ai datelor, existenţa drepturilor prevăzute de Legea privind protecţia datelor cu caracter personal, precum şi condiţiile în care pot fi exercitate.

9.2. Dreptul de acces la date, constă în dreptul de a obţine de la IMSP SCR „Timofei Moşneaga" în temeiul unei cereri, confirmarea/infirmarea faptului dacă datele cu caracter personal care-l vizează au fost sau nu prelucrate precum şi a informaţiilor ce vizează dreptul la informare.

9.3. Dreptul de intervenţie constă în dreptul de a obţine în baza unei cereri, rectificarea, actualizarea, blocarea, ştergerea sau transformarea în date anonime a datelor a căror prelucrare nu este conformă cu cerinţele Legii privind protecţia datelor cu caracter personal, în special, a datelor incomplete sau inexacte.

9.4. Dreptul de opoziţie constă în dreptul de a se opune în orice moment, din motive întemeiate şi legitime legate de situaţia sa particulară, că datele care îl vizează să facă obiectul unei prelucrări, cu excepţia cazurilor în care există dispoziţii legale care prevăd altfel.

9.5. Dreptul de a nu fi supus unei decizii individuale, constă în dreptul de a cere şi de a obţine retragerea, anularea sau reevaluarea oricărei decizii care produce efecte juridice în privinţa subiectului de date cu caracter personal, adoptată exclusiv pe baza unei prelucrări automatizate de date, destinată să evalueze unele aspecte ale personalităţii sale, precum competenţa profesională, credibilitatea, comportamentul ori alte asemenea aspecte.

X. Securitatea mediului fizic şi autorizarea accesului în procesul prelucrării datelor cu caracter personal.

10.1. Autorizarea accesului fizic:

a) tot personalul medical şi auxiliar este obligat să poarte ecusoane, în care să fie indicat numele, prenumele, funcţia, denumirea instituţiei. Permisul este sursa de informare cu privire la partenerul de dialog şi serveşte drept legitimaţie de serviciu;

b) accesul în sediile/oficiile/birourile ori spaţiile unde sunt stocate purtători de date cu caracter personal (fişe medicale, registre, liste, certificate, concluzii consultative, protocoale ale explorărilor de laborator şi diagnostice, alte feluri de

formulare medicale, note informative, recenzii etc.) este restricționat, fiind permis doar persoanelor, care au autorizația necesară (funcția cărora prevede), conform listei și cu prezența ecusonului și doar în timpul orelor de program,

10.2. Șefii de secții, precum și toate persoanele responsabile, conform obligațiunilor personale, efectuează administrarea și monitorizarea accesului fizic în toate punctele de acces la sistemele informaționale de date cu caracter personal, în birouri, oficii și încăperi respective, inclusiv se reacționează la încălcarea regimului de acces. Înainte de acordarea accesului fizic la date de caracter personal, persoanele responsabile de protecție și păstrare verifică competențele de acces.

10.3. Perimetrul de securitate se determină ca perimetrul încăperii și trebuie să fie integru din punct de vedere fizic.

10.4. În cazul amplasării încăperilor la parter și/sau la ultimul etaj al clădirii, precum și în cazul existenței scărilor antiincendiare, la ferestrele încăperilor respective se instalează gratii.

10.5. Agendele și/sau cărțile de telefoane în care se conțin indicii despre locul amplasării mijloacelor de prelucrare a datelor cu caracter personal nu vor fi accesibile persoanelor străine.

10.6. Șefii de servicii, subdiviziuni, personalul medical la locul de muncă trebuie să organizeze plasarea obiectelor ce conțin date cu caracter personal în așa mod ca să răspundă necesității asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri.

10.7. Folosirea tehnicii foto, video, audio sau altor mijloace de înregistrare în perimetrul de securitate (registraturile, secțiile, subdiviziunile, arhiva instituției), este admisă doar în cazul prezenței unei permisiuni speciale a administrației IMSP SCR „Timofei Moșneaga".

10.8. Purtătorii de informații (fișe, registre, formulare, concluzii consultative, protocoale ale explorărilor etc.) și mijloacele de prelucrare a datelor cu caracter personal (stații de lucru, CD/DVD-uri, stik-uri de memorie) scoase din încăperile aflate în perimetrul de securitate nu trebuie lăsate fără supraveghere în locuri publice.

10.9. Să asigure controlul accesului fizic al vizitatorilor în încăperile unde sunt amplasate sistemele informaționale de date cu caracter personal (servere). Accesul vizitatorilor se înregistrează în registre, care se păstrează 3 ani, ulterior fiind transmise în arhivă.

10.10. Vizitatorii sediilor/oficiilor/birourilor ori spațiilor unde sunt stocate purtători de date cu caracter personal (revizori, experți, cursanți, precum și lăcătuși, lucrători auxiliari, etc.) trebuie să fie însoțiți de persoane împuternicite în asemenea scop, cu exercitarea în paralel a controlului asupra acțiunilor acestora.

10.11. În încăperile unde sunt amplasate documentația medicală și a personalului instituției, sistemele informaționale de date cu caracter personal, mijloacele de prelucrare a datelor cu caracter personal, sunt prevăzute mijloace de asigurare a securității antiincendiare.

10.12. Suplimentar în instituție este implementat sistemul automatizat de depistare/semnalizare a incendiilor în sediile/oficiile/birourile unde este stocată documentația medicală și alți purtători cu date personale

XI. Măsurile generale de administrare a securității informaționale

11.1. Se asigură securitatea echipamentului electric utilizat pentru menținerea funcționalității sistemelor informaționale de date cu caracter personal, a cablurilor electrice, inclusiv protecția acestora contra deteriorărilor și conectărilor nesancționate.

11.2. În cazul apariției situațiilor excepționale, de avarie sau de forță majoră, este asigurată posibilitatea deconectării electricității la sistemele informaționale de date cu caracter personal, inclusiv posibilitatea deconectării oricărui component TI.

11.3. În cazul neutilizării temporare a purtătorilor de informație pe suport de hârtie sau electronic, care conțin date cu caracter personal, acestea se păstrează în safeuri sau dulapuri metalice care se încuie.

11.4. Computerele, terminalele de acces și imprimantele sunt deconectate la terminarea sesiunilor de lucru.

11.5. Trebuie administrat accesul fizic la mijloacele de reprezentare a informației, care conține date cu caracter personal, în scopul împiedicării vizualizării acesteia de către persoane neautorizate.

11.6. Scoaterea și introducerea mijloacelor de prelucrare a datelor cu caracter personal din/în perimetrul de securitate se înregistrează.

11.7. Accesul fizic la mijloacele de reprezentare a informației care conține date cu caracter personal, în scopul împiedicării vizualizării acesteia de către persoane neautorizate este interzis și controlat.

11.8. Mijloacele de prelucrare a datelor cu caracter personal, informația care conține date cu caracter personal sau soft-urile destinate prelucrării datelor cu caracter personal sunt scoase din perimetrul de securitate doar în temeiul unei permisiuni scrise a conducerii IMSP SCR „Timofei Moșneaga".

11.9. Pentru toate categoriile sistemelor informaționale de date cu caracter personal se implementează mecanisme de înregistrare și evidență a persoanelor care au acces sau participă la operațiunile de prelucrare a datelor cu caracter personal și care, în caz de necesitate, permit identificarea cazurilor neautorizate de acces sau de prelucrare ilegală a datelor cu caracter personal.

11.10. Pentru toate categoriile sistemelor informaționale de date cu caracter personal:

a) este autorizat accesul la sistemele informaționale de date cu caracter personal în conformitate cu politica de administrare a accesului stabilită de deținătorul de date cu caracter personal;

b) accesul la funcțiile de securitate ale sistemelor informaționale de date cu caracter personal și la datele acestora este acordat doar persoanelor responsabile indicate expres în politica de securitate a deținătorului de date cu caracter personal.

11.11. Drepturile de acces al utilizatorilor la sistemele informaționale de date cu caracter personal sunt revizuite la necesitate, în cazul modificărilor organizatorice sau în logistica acordării serviciilor medicale.

11.12. Administrația IMSP SCR „Timofei Moșneaga" autorizează realizarea fluxurilor informaționale în procesul transmiterii acestora în interiorul și în afara sistemelor informaționale de date cu caracter personal.

11.13. Repartizarea obligațiilor subiecților care asigură funcționarea sistemelor informaționale de date cu caracter personal este efectuată prin intermediul învestirii cu drepturi/competente corespunzătoare de acces, printr-un act administrativ al conducerii deținătorului de date cu caracter personal.

11.14. Utilizatorii sistemelor informaționale de date cu caracter personal se învestesc doar cu acele drepturi/competente, care sunt necesare pentru realizarea de către ei a obiectivelor stabilite acestora.

11.15. Pentru toate categoriile sistemelor informaționale de date cu caracter personal se efectuează monitorizarea permanentă și analiza înregistrărilor de audit a securității în sistemele informaționale de date cu caracter personal, în scopul depistării activităților neobișnuite sau suspecte de utilizare a acestor sisteme informaționale, cu întocmirea raportului referitor la cazurile depistării acestor activități, stocate în mijloacele electronice de calcul și întreprinderea acțiunilor prestabilite în politica de securitate pentru astfel de cazuri.

11.16. Rezultatele auditului securității în sistemele informaționale de date cu caracter personal, care reprezintă operațiuni de prelucrare a datelor cu caracter personal și mijloacele de efectuare a auditului, se protejează contra accesului neautorizat prin instituirea măsurilor de securitate adecvate, inclusiv prin asigurarea confidențialității și integrității acestora.

11.17. Durata stocării rezultatelor auditului securității în sistemele informaționale de date cu caracter personal se justifică în politica de securitate a datelor cu caracter personal, dar în orice caz acest termen nu este mai mic de 3 ani, pentru a fi posibil folosirea acestora în calitate de probe în cazul incidentelor de securitate, unor eventuale investigații sau procese judiciare. În cazul în care investigările sau procesele judiciare se prelungesc, rezultatele auditului se păstrează pe toată durata acestora.

XII. Dispoziții finale

12.1. Politica de securitate a datelor cu caracter personal se revizuiește periodic, ca rezultat al modificărilor sau reevaluării și se aprobă de directorul instituției.

12.2. Documentul este adus la cunoștința utilizatorilor și salariaților din cadrul IMSP SCR „Timofei Moșneaga", în limitele competențelor funcționale și nivelului de acces.

Director interimar **Andrei UNCUȚA**