INSTITUŢIA MEDICO-SANITARĂ PUBLICĂ „SPITALUL CLINIC AL MINISTERULUI SĂNĂTĂŢII”

ORDIN Nr.__75__

mun.Chişinău

„_12_” ____04_____20_16__

„Cu privire la protecţia datelor
cu caracter personal "

Întru asigurarea protecţiei datelor cu caracter personal în conformitate cu Legea nr.133 din 18.07.2011 ”Privind protecţia datelor cu caracter personal”, HG RM nr. 1123 din 14.12.2010 ”Privind aprobarea cerinţelor faţă de asigurarea securităţii datelor cu caracter personal”, reeșind din cerințele actuale a actelor legislative și normative.

ORDON :

I. Aprob următoarele Regulamente :

I.1. Privind asigurarea securităţii datelor medicale cu caracter personal în cadrul IMSP "Spitalul Clinic al Ministerului Sănătății" ***Anexa1.***

I.1.1. Acord informațional pentru efectuarea intervenției medicale cu lista intervențiilor ***Anexa1.1***

I.1.2. Consimțământul pacientului despre prelucrarea datelor cu caracter personal privind starea de sănătate ***Anexa1.2***

I.1.3. Formularul de consimțământ informat ***Anexa1.3***

I.1.4. Acordul pacientului pentru transuzia sîngelui și componentelor de sînge de la donatori ***Anexa1.4***

I.2. Privind asigurarea securităţii datelor cu caracter personal (medical), prelucrare acestora în mod manual(pe suport de hârtie) în IMSP "Spitalul Clinic al Ministerului Sănătății" ***Anexa2.***

I.2.1. Acord informațional la intevenții medicală contra plată ***Anexa2.1***

I.3. Cu privire la protecţia datelor cu caracter personal, prelucrare cu utilizarea tehnologiilor informaţionale în IMSP ”Spitalul Clinic al Ministerului Sănătății” ***Anexa3.***

I.4. Cu privire la protecţia datelor cu caracter personal În serviciul resurse umane ***Anexa4*.**

I.5. Privind asigurarea securităţii datelor cu caracter personal a pacientului în cadrul IMSP "Spitalul Clinic al Ministerului Sănătății" ***Anexa5.***

I.6. Cu privire la asigurarea securităţii datelor cu caracter personal pentru Sistemul Informaţional de Evidenţă a Pacienţilor din Staţionar în cadrul IMSP "Spitalul Clinic al Ministerului Sănătății" ***Anexa6.***

I.7. Cu privire la supravigherea mijloacelor video. ***Anexa7.***

II. Se desecmnează funcțiile persoanelor responsabile privind asigurarea securității datelor medicale cu caracter personal, prelucrarea acestora cu utilizarea tehnologiilor informaționale și în mod manual (pe suport de hîrtie):

Funția	**Subdiviziunile**
Șef(a),administrator BD	Scția informatică și statistică medicală
Sef de secție, Asistenta Superioară	Secția Boli Interne-1
Sef de secție, Asistenta Superioară	Secția Boli Interne-2
Sef de secție, Asistenta Superioară	Secția Gereatrie
Sef de secție, Asistenta Superioară	Secția Boli Interne-4
Sef de secție, Asistenta Superioară	Secția Neurologie
Sef de secție, Asistenta Superioară	Secția Chirurgie
Sef de secție, Asistenta Superioară	Secția Internare
Sef de secție, Asistenta Superioară	Secția Anestezie și reanimare
Șef Centru N.G.G	Centrul Național G.G.
Sef de secție, Asistenta Superioară	Secția Consultativ Diagnostic
Sef CMF, Asistenta Superioară	Secția Centrul Medecină Primară
Sef CMS, Asistenta Superioară	Centrul Medical Specializat
Sef de secție, Asistenta Superioară	Secția Fizioterapie și Recuperare
Farmacist diriginte	Farmacie
Sef de laborator, Laborant Superior	Laborator Clinic
Sef Serviciu R.I., Tehnician Radiolog	Serviciul Radiologie și imagistică
Medic Diagnostic funcțoinal	Serviciul Diagnostic funțional cardiologie
Sef Serviciu Diagnostic funcțoinal	Serviciul Diagnostic funțional neurologie
Sef de secție, Asistenta Superioară	Secția Stomatologie
Sef de secție, Asistenta Superioară	Secția Ortopedie
Sef de serviciu Ginecologic	Serviciul Ginecologie

II.1. Persoanele responsabile în activitatea sa vor respecta întocmai cerițelor prevăzute în regulamentele I.1, I.2, I.3, I.5, I.6.

II.1.1. Vor organiza instuirea subalternilor referitor la cunoașterea categoriilor de date cu caracter personal și cerințelor de protecție a acestora, cît și persoanelor noi angajate cu înregestrarea în registru special.

II.2. Se numește persoana responsabilă privind protecția datelor cu caracter personal a colaboratorilor în serviciul personal –sefa serviciului personal.

II.2.1. V-a semna cu salariații din IMSP ”SCMS”, ”Consimțământul salariatului privind obținerea, păstrarea, prelucrarea și protecția datelor cu caracter personal”.

II.2.2. V-a întreprinde acțiuni privind modificarea de rigoare în conformitate cu cerințele ordinului dat în regulamentele de activitate a subdiviziunilor și Fișilor de Post a colaboratorilor.

II.2.3. În activitatea s-a se va călăuzi de cerințele Regulamentelor I.1, I.4, I.6.

II.3. Se numește persoana responsabilă privind asigurarea securității datelor cu caracter personal pentru SIA ”1C” contabil-șef. **Anexa 3.**

II.3.1. V-a întocmi DECLARAȚIE DE CONFIDENȚIALITATE cu toți utilizatorii care au acces la SIA ”1C”.

II.4. Se numește persoana responsabilă privind asigurarea securității, păstrarea și eliberarea datelor cu caracter personal în mod manual : Registratura serviciul ambulatoriu**.**

II.5. Registratorul serviciului stomatologic**.**

II.6. Registratorul Secția Fizioterapie și Recuperare**.**

II.7. Arhivariul IMSP ”SCMS”**.**

II.8. V-or elabora Registru special pentru înregestrarea fișelor medicale eliberate și scoase din instituție.

II.9. Controlul asupra executării prezentului ordin se atribuie vice-directorilor d-ul V.Parasca, dna. M. Țiberneac.

DIRECTOR **Gheorghe ȚURCANU**

Anexa 1

La ord. nr.___ din _____

Regulamentul privind asigurarea securităţii datelor medicale cu caracter personal în cadrul IMSP "Spitalul Clinic al Ministerului Sănătății"

I. Dispoziţii generale

1.1. Regulamentul cu privire la asigurarea securităţii datelor medicale cu caracter personal stabileşte reguli de implementare a măsurilor organizatorice, tehnice în cadrul instituţiei, responsabilităţile personalului în sistemul de management al protecţiei datelor medicale cu caracter personal.

1.2. Regulamentul dat este elaborat în temeiul următoarelor acte legislative şi normative în domeniu:
- Legea №411-XIII din 28.03.1995 „Legea ocrotirii sănătăţii”, cu ulterioarele modificări.
- Legea №264 din 27.10.2005 „Privind exercitarea profesiunii de medic”;
- Legea №263 din 27.10.2005 „Cu privire la drepturile şi responsabilităţile pacientului”;
- Legea №133 din 08.07.2011 „Privind protecţia datelor cu caracter personal”
- Legea №982-XIV din 11 mai 2000 „Cu privire la accesul la informaţie”
- Legea №23 din 16.02.20.07 „Cu privire la profilaxia infecţiei HIV/SIDA”;
- Legea №10 din 03.02.2009 „Privind supravegherea de stat a sănătăţii publice”;
- Legea №100-XV din 26.04.2001 „Privind actele de stare civilă”
- Legea №105-XV din 13.03.2003 „Privind protecţia consumatorilor”
- Legea №467-XV din 21.11.2003 „Cu privire la informatizare şi resursele informaţionale de stat;
- Legea №190- XIII din 19.07.1994 „Cu privire la petiţionare”
- Legea №1585–XIII din 27.02.1998 „Cu privire la asigurarea obligatorie de asistenţă medicală”
- Codul Contravenţional al RM;
- Codul Muncii al RM;
- Hotărârea Guvernului Republicii Moldova №663 din 23.07.2010 „Pentru aprobarea Regulamentului sanitar privind condiţiile de igienă pentru instituţiile medico-sanitare”;
- Hotărârea Guvernului Republicii Moldova №1128 din 24.10.2003 ”Cu privire la aprobarea Concepţiei „Sistemului Informaţional Medical Integrat”;
- Hotărârea Guvernului Republicii Moldova №562 din 22.05.2006 „Cu privire la crearea sistemelor şi resurselor informaţionale automatizate de stat”;
- Hotărârea Guvernului Republicii Moldova №1123 din 14.12.2010 „Privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal”;
- Hotărârea Guvernului Republicii Moldova №296 din 15.05.2012 „Privind aprobarea Regulamentului Registrului de evidenţă a operatorilor de date cu caracter personal”;
- Ordinul Ministerului Sănătăţii №239 din 04.08.2005 „Despre introducerea sistemului de expertiză a produselor de program şi a bazelor de date, utilizate în instituţiile medico-sanitare publice din Republica Moldova”.

1.3 Regulile obligatorii ce se vor aplica în toate subdiviziunile instituţiei care dispun de sisteme informaţionale şi date cu caracter personal prin asigurarea următoarelor acţiuni:
- controlul strict asupra accesului la informaţie;

- accesul autorizat al utilizatorului;
- prevenirea compromiterii sau furtului de informaţii şi a sistemelor de procesare a informaţiilor;
- prevenirea accesului neautorizat la serviciile de reţea;
- prevenirea accesului neautorizat la sistemele de operare;
- prevenirea accesului neautorizat la informaţia deţinută în sistemele de aplicaţii;
- protecţia serviciilor interconectate (LAN, WAN, INTERNET);
- securitatea informaţiei, atunci când se folosesc sisteme pentru prelucrarea datelor cu caracter personal şi medical în mod manual;

1.4 Deţinătorii de informaţii sunt toţi salariaţii IMSP "SCMS".

II. Organizarea măsurilor de protecţie a datelor medicale cu caracter personal

2.1. Documentaţia medicală, inclusiv fişele medicale (forma 003/e cu toate anexele, 066/e, 001/e, 014/e, 015/e, 027/e, 013/e, 044/e, 036/e) a pacienţilor înregistraţi în cadrul spitalului, inclusiv alte formulare şi registre, care conţin date cu caracter personal şi medical - se consideră purtătoare de date cu caracter personal.

2.2. Această documentaţie urmează a fi păstrată de angajaţii instituţiei în birouri şi spaţii special destinate (arhivă, statistică, birouri ale medicilor şi asistentelor medicale, cabinete diagnostice, laboratoare).

2.3. Fişele medicale (forma 003/e, cu toate anexele, 066/e, 001/e, 014/e, 015/e, 027/e, 013/e, 044/e, 036/e) după externarea pacienţilor sunt păstrate în arhiva spitalului, în conformitate cu cerinţele documentaţiei de directivă în vigoare.

2.4. Transmiterea fişelor medicale în alte secţii, cabinete, se asigură numai prin personalul medical şi auxiliar responsabil.

2.5. Nu se permite eliberarea fişelor medicale în original pacienţilor (reprezentanţilor acestora ş.a.).

2.6. Familiarizarea pacientului (reprezentantului acestuia) despre datele cu caracter personal şi medical se execută în corespundere cu actele normative în vigoare, la cererea lui şi nu poate fi realizată prin eliberarea fişei medicale în original pacientului.

2.7. În cazurile prevăzute de actele normative în vigoare fişele medicale, pot fi eliberate (scoase din instituţie) numai cu înregistrarea acestui fapt în registrul special al arhivei instituţiei sub semnătură personală.

2.8. În scopul evitării divulgării datelor cu caracter personal şi medical se cere obligatoriu, stabilirea identităţii persoanei care recepţionează fişele medicale prin verificarea buletinului de identitate, legitimaţiei de serviciu et c.

2.9. Nu se permite discuţii prin telefon referitor la datele cu caracter personal şi medical.

III. Consimţământul la prelucrarea datelor cu caracter personal şi medical

3.1. Datele cu caracter personal şi medical al beneficiarilor de servicii prestate în cadrul IMSP "SCMS" pot fi prelucrate numai cu consimţământul acestora.

3.2 Consimţământul pentru prelucrarea datelor privind starea de sănătate se obţine prin completarea unui acord informat (anexa №1 al ordinului intern).

3.3.Prelucrarea datelor cu caracter personal referitor la pacient se efectuează cu consimţământul lui, cu excepţia cazurilor prevăzute de legislaţia în vigoare. Modelul consimţământului este ataşat la fişa medicală a pacientului internat.

3.4 Familiarizarea beneficiarilor de servicii medicale, inclusiv rudelor acestora, referitor la scopul şi efectele consimţământului se efectuează de către şefii de secţii medicii ordinatori, medicii de gardă.

IV. Securitatea datelor cu caracter personal şi medical de către angajaţii instituţiei

4.1. Vicedirectorii, şefii de secţii şi servicii, reieşind din specificul activităţii, organizează măsurile de securitatea a datelor cu caracter personal, inclusiv procedurile şi măsurile legate de realizarea acestui regulament, cu aplicarea soluţiilor practice.
4.2. Salariaţii instituţiei sunt instruiţi referitor la cunoaşterea categoriilor de date cu caracter personal supuse prelucrării, cerinţele de protecţie a acestora şi principiile operaţiunilor de prelucrare efectuate asupra lor.
Responsabili de instruire sunt şefii secţiilor (la angajare – instruire primară), iar juristul, vicedirectorii, periodic, la necesitate.
4.3. Salariaţii efectuează prelucrarea datelor cu caracter personal conform atribuţiilor funcţionale. Nu se admite prelucrarea datelor cu caracter personal în alte scopuri, decât în scopul exercitării obligaţiunilor funcţionale.
4.4. ***Responsabilităţile şefiilor de secţii şi servicii şi utilizatorilor datelor cu caracter personal***

- Colaboratorii spitalului implicaţi în înregistrarea, transmiterea, recepţionarea, păstrarea, eliberarea datelor medicale şi generale cu caracter personal poartă responsabilitate personală pentru încălcările comise.
- Şefii secţiilor, subdiviziunilor, asistentele medicale şi cele superioare poartă responsabilitate pentru organizarea şi controlul măsurilor contra divulgării, prelucrării neautorizate, distrugerii, denaturării, furtului, pierderii actelor medicale sau încălcarea confidenţialităţii datelor cu caracter personal.
- Nu se admite divulgarea datelor medicale cu caracter personal persoanelor terţe, prin telefon sau prin comunicare directă fără stabilirea identităţii persoanei şi a temeiului legal al solicitării.
- Nu se admite divulgarea datelor medicale cu caracter personal în discuţii dintre salariaţi, cu excepţia cazurilor de necesitate de serviciu.
- Personalul medical este obligat să explice pacienţilor, solicitanţilor motivele nedivulgării datelor medicale cu caracter personal, sau refuzul eliberării extraselor, fişelor, certificatelor etc.
- Utilizatorii datelor medicale cu caracter personal din spital, vor semna angajament de confidenţialitate (nedivulgarea neautorizată a datelor cu caracter personal şi medical prin fişa de post.)

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

5.1. Tot personalul medical şi auxiliar este obligat să poarte permis nominal la locul de muncă, în care să fie indicat numele, prenumele, funcţia, denumirea instituţiei, fotografia. Permisul este sursa de informare cu privire la partenerul de dialog şi serveşte drept legitimaţie de serviciu.
5.2. 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 restricţionat, fiind permis doar persoanelor care au autorizaţia necesară (funcţia cărora prevede) şi doar în timpul orelor de program, conform listei şi permisului;
5.3. Şefii de secţii şi servicii, precum şi toate persoanele responsabile, conform obligaţiunilor persoanele, efectuează administrarea şi monitorizarea accesului fizic în toate punctele de acces la sistemele informaţionale de date cu caracter personal, în birouri, oficii şi încăperi respective, şi reacţionează la încălcarea regimului de acces. Înainte de acordarea accesului fizic la date de caracter personal, persoanele responsabile de protecţie şi păstrare verifică competenţele de acces.
5.4. Perimetrul de securitate se determină ca perimetrul încăperii şi trebuie să fie integru din punct de vedere fizic.
5.5. Computerele, serverele, alte terminale de acces sunt amplasate în locuri cu acces limitat pentru persoane străine.
5.6. Şefii de servicii, personalul medical la locul de muncă trebuie să organizeze plasarea obiectelor ce conţin date cu caracter personal în aşa mod ca să răspundă necesităţii asigurării securităţii acestora contra accesului nesancţionat, furturilor, incendiilor, inundaţiilor şi altor posibile riscuri.
5.7. Folosirea tehnicii foto, video, audio sau altor mijloace de înregistrare în perimetrul de securitate (departamentul informţional al secţiei Internări, arhiva instituţiei), este admisă doar în cazul prezenţei unei permisiuni speciale a administraţiei IMSP "SCMS".
5.8. Se asigură controlul accesului fizic al vizitatorilor în încăperile unde sunt amplasate sistemele informaţionale de date cu caracter personal (servere). Accesul vizitatorilor se înregistrează în registre, care se păstrează 3 ani, ulterior fiind transmise în arhivă.

VI. Asigurarea securităţii antiincendiare a sistemelor informaţionale de date medicale cu caracter personal.

6.1. În încăperile unde este amplasată documentaţia medicală a instituţiei, sistemele informaţionale de date cu caracter personal, mijloacele de prelucrare a datelor cu caracter personal, sunt prevăzute mijloace de asigurare a securităţii antiincendiare.
6.2. Suplimentar, anual, instituţia se supune verificării privind funcţionarea securităţii antiincendiare în birourile unde este stocată documentaţia medicală şi alte feluri de purtători de date cu caracter personale.

VII. DISPOZIŢII FINALE

7.1. Prezentul Regulament intră în vigoare din data aprobării lui prin ordinul IMSP SCMS.

7.2. Modificarea şi completarea Regulamentului în cauză se efectuează în corespundere cu actele normative în vigoare.

Anexa nr. 2
la Ordinul MS
nr.303 din 06.05.2010

Lista intervenţiilor medicale
care necesită perfectarea acordului informat al pacientului

I. Intervenţiile chirurgicale, inclusiv manopere de mică chirurgie.
II. Intervenţii parenterale, inclusiv imunizări.
III. Servicii medicale specifice:
a) Prelevarea singelui pentru determinarea parametrilor clinici, biochimici,
imunologici, serologici;
b) Recoltarea produselor pentru biopsie, citologie, histologie;
c) Extracţie de corpi străini;
d) Tratamente locale (badijonaj, lavaj);
e) Manopere terapeutice (puncţia, cateterizarea).
IV. Servicii medicale paraclinice, inclusiv:
a) Testele intradermale;
b) Servicii de transfuzie;
c) Servicii medicale de diagnostic funcţional (cu test farmacologic, de
efort sau funcţional, etc);
d) d. Imagistica medicala (metode invazive de diagnostic cu ghidaj ecografic; ecografia cardiaca (ecocardiografie) cu efort fizic, farmacologic, cu contrast, transesofagiană);
e) Investigaţii de radiodiagnostic;
f) Tomografia convenţionala si computerizata;
g) Investigaţii angiografice; Medicina nucleara;
h) Investigaţii prin rezonanta magnetica-nucleara (RMN);
i) Investigaţii de diagnostic intraarticulare;
j) Endoscopia de diagnostic
V. Servicii de fizioterapie si reabilitare medicala cu metode fizice, inclusiv:
a) Electroterapia;
b) b. Aerosolo - si electro-aerosoloterapia;
c) c. Fototerapia;
VI. Tratamente terapeutice cu efecte adverse specifice sau risc sporit
In dependenţă de profilul de activitate a instituţiei medico-sanitare, lista
intervenţiilor medicale, care necesita perfectarea acordului informat al pacientului,
se completează prin ordin intern.

Anexa nr. 3
la Ordinul MS
nr.303 din 06.05.2010

Acordului informat la intervenţia medicală

Instituţia medico-sanitară publică _____ _____
Eu, subsemnatul _____ prin prezentul imi exprim acordul (consimţământul) la următoarele proceduri de diagnostic/tratament prin următoarele metode: _____
_____
_____
caracterul si scopul cărora mi-au fost explicate si propuse de către medicul,_____
Eu am fost informat si am inţeles ca aceste metode sunt efectuate prin utilizarea dispozitivelor (aparatelor) _____,
special destinate metodelor propuse de diagnostic/tratament. Procedurile vor fi efectuate la recomandarea medicului de către asistentele medicale, special pregătite in acest domeniu. In cadrul efectuării procedurilor de tratament eu voi fi conectat la aparatul (dispozitivul) medical prin intermediul _____
si voi avea senzaţii _____
(vibraţie, mici inţepături, căldură, caracteristice acestor forme de tratament).
Mie mi s-a explicat despre beneficiile acestor metode de diagnostic si tratament, care nu au un grad absolut de eficacitate si despre consecinţele nedorite ce pot duce in anumite cazuri rare la complicaţii grave si chiar moarte. Vor fi luate toate masurile de preintampinare care constau in supravegherea atenta a stării mele de către personalul medical mediu in procesul tratamentului, iar utilajul si medicamentele necesare pentru acordarea asistenţei medicale de urgenţă sunt disponibile.

Eu am inţeles tot ce mi-a explicat medicul şi am primit răspuns la toate intrebările mele.
Benevol imi exprim consimţământul conştient pentru efectuarea procedurilor descrise contra plată şi pentru colectarea, stocarea, utilizarea şi transmiterea informaţiei de sănătate. Concomitent îmi asum responsabilitatea pentru orice incălcare a regulilor de comportament si neindeplinirea recomandărilor primite.

Data _____ Semnătura pacientului (reprezentantului legal) _____

Confirm, ca eu am explicat pacientului caracterul, scopul, beneficiile si riscurile procedurilor descrise.

Data _____ Semnătura medicului _____

Documentaţie medicală
aprobată prin ordinul IMSP "SC MS"

nr.___

din „_____”_____201

INSTITUŢIA MEDICO-SANITARĂ PUBLICĂ „SPITALUL CLINIC AL MINISTERULUI SĂNĂTĂŢII”

ACORDUL INFORMAT LA INTERVENŢIA MEDICALĂ

Eu subsemnatul(ă) _____ prin prezentul îmi exprim acordul (consimţământul) la efectuarea:

1. examenului medical (inclusiv) conform ordinului MS RM Nr. 132 din 17.06.1996)
2. intervenţiilor medicale
3. recoltării, folosirii tuturor produselor biologice
4. fotografierii, filmării
5. diagnosticului funcţional (ECG, FRE, dinamometrie, proba la rece, examinarea aparatului vestibular, audiometrie)

Eu am fost informat/ă şi am înţeles că unele metode sunt efectuate prin utilizarea dispozitivelor special destinate metodelor de diagnostic. Procedurile vor fi efectuate la recomandarea medicului de către asistentele medicale, special pregătite în acest domeniu. În cadrul efectuării procedurilor de diagnostic eu voi fi conectat/ă la aparate, funcţia cărora mie mi s-a explicat. De asemenea, mie mi s-a explicat despre acestea metode de diagnostic, care nu au un grad absolut de eficacitate şi despre consecinţele nedorite ce pot duce în anumite cazuri rare la complicaţii grave şi chiar moarte. Vor fi luate toate măsurile de preîntâmpinare, care costau în supravegherea atentă a stării mele de către personalul medical mediu, iar utilajul şi medicamente necesare pentru acordarea asistenţei medicale de urgenţă sunt disponibile. Eu am înţeles totul ce mi-a explicat medicul şi am primit răspuns la toate întrebările mele. Benevol îmi exprim consimţământul conştient pentru efectuarea investigaţiilor descrise contra plată şi pentru colectarea, stocarea, utilizarea şi transmiterea informaţiei de sănătate. Concomitent îmi asum responsabilitatea pentru orice încălcare a regulilor de comportament şi neîndeplinirea recomandărilor primite.

Declar pe proprie răspundere, că:

- nu sunt la evidenţă cu epilepsie, boli psihice, boli neurologice, maladii cardiovasculare, maladii ale aparatului respirator şi renal, tuberculoză, hepatite virale, SIDA;
- nu sunt sub tratament pentru boli neuropsihice, tuberculoză şi diabet;
- nu sunt la evidenţa medicului oncolog, maladii oncologice şi hematologice neg;
- nu sunt la evidenţa medicului narcolog, dermatovenerolog, maladii sexual transmisibile.

Accept tratamentul şi investigaţiile adăugătoare pentru precizarea maladiilor depistate în urma examenului medical:

- contra plată în IMSP "SC MS", sau
- conform poliţei de asigurare pe locul de trai.

Data”_____”_____20___

Semnătura medicului _____ **Semnătura pacientului _____**

Documentaţie medicală
aprobată prin ordinul IMSP "SC MS"

nr.___

din „_____”_____201

INSTITUŢIA MEDICO-SANITARĂ PUBLICĂ „SPITALUL CLINIC AL MINISTERULUI SĂNĂTĂŢII”

ACORDUL INFORMAT LA INTERVENŢIA MEDICALĂ

Eu subsemnatul(ă) _____ prin prezentul îmi exprim acordul (consimţământul) la efectuarea:

6. examenului medical (inclusiv) conform ordinului MS RM Nr. 132 din 17.06.1996)
7. intervenţiilor medicale
8. recoltării, folosirii tuturor produselor biologice
9. fotografierii, filmării
10. diagnosticului funcţional (ECG, FRE, dinamometrie, proba la rece, examinarea aparatului vestibular, audiometrie)

Eu am fost informat/ă şi am înţeles că unele metode sunt efectuate prin utilizarea dispozitivelor special destinate metodelor de diagnostic. Procedurile vor fi efectuate la recomandarea medicului de către asistentele medicale, special pregătite în acest domeniu. În cadrul efectuării procedurilor de diagnostic eu voi fi conectat/ă la aparate, funcţia cărora mie mi s-a explicat. De asemenea, mie mi s-a explicat despre acestea metode de diagnostic, care nu au un grad absolut de eficacitate şi despre consecinţele nedorite ce pot duce în anumite cazuri rare la complicaţii grave şi chiar moarte. Vor fi luate toate măsurile de preîntâmpinare, care costau în supravegherea atentă a stării mele de către personalul medical mediu, iar utilajul şi medicamente necesare pentru acordarea asistenţei medicale de urgenţă sunt disponibile. Eu am înţeles totul ce mi-a explicat medicul şi am primit răspuns la toate întrebările mele. Benevol îmi exprim consimţământul conştient pentru efectuarea investigaţiilor descrise contra plată şi pentru colectarea, stocarea, utilizarea şi transmiterea informaţiei de sănătate. Concomitent îmi asum responsabilitatea pentru orice încălcare a regulilor de comportament şi neîndeplinirea recomandărilor primite.

Declar pe proprie răspundere, că:

- nu sunt la evidenţă cu epilepsie, boli psihice, boli neurologice, maladii cardiovasculare, maladii ale aparatului respirator şi renal, tuberculoză, hepatite virale, SIDA;
- nu sunt sub tratament pentru boli neuropsihice, tuberculoză şi diabet;

- nu sunt la evidenţa medicului oncolog, maladii oncologice şi hematologice neg;
- nu sunt la evidenţa medicului narcolog, dermatovenerolog, maladii sexual transmisibile.

Accept tratamentul şi investigaţiile adăugătoare pentru precizarea maladiilor depistate în urma examenului medical:
- contra plată în IMSP "SC MS", sau
- conform poliţei de asigurare pe locul de trai.

Data”_____ ”_____20___

Semnătura medicului _____ **Semnătura pacientului _____**

FORMULARUL DE CONSIMTAMANT INFORMAT

1. Eu……. născut la data

   de…….

   în…… accept de bună-voie sa iau parte la un studiu

   clinic

   codul…….

   titlu……..

2. Mi s-a dat o explicaţie completa cu privire la natura, scopul si durata probabila a studiului si la ceea
   ce va trebui sa fac, si am fost avertizat in legătură cu orice risc, discomfort sau posibile efecte
   adverse asupra sanatatii sau stării mele de bine, care crede ca ar putea rezulta.
3. Am citit, Formularul de Consimtamant. Informat pentru acest studiu. L-am semnat si datat personal in doua exemplare.
4. Mi s-a oferit ocazia de a întreba pe Doctorul/ii studiului despre toate aspectele studiului, pana cand le-am Înţeles pe deplin.
5. Sunt de acord in mod voluntar sa particip la studiul de bioechivalenta a medicamentului menţionat mai sus si am fost informat ca pot refuza sa particip sau sa ma retrag din studiu in orice moment.
6. Sunt de acord ca informaţiile mele personale sa fie pastrate in înregistrările Centrului Clinic sau in baza de date a Investigatorului Clinic IMSP ”SCMS”.
7. Mi s-a spus si înţeleg ca acest studiu nu este efectuat pentru beneficiul meu, ci doar pentru cercetare si achiziţionarea de cunoştinţe medicale si ca acest studiu a fost analizat de către un Comitet Etic.
8. Sunt de acord sa urmez instrucţiunile, sa cooperez cu Medicul Studiului cu încredere si sa o
   informez imediat in legătură cu orice problema de sanatate sau modificări in starea mea de bine.
9. Am fost informat ca in cazul oricărei deteriorări a sanatatii mele care are legătură cu studiul voi primi îngrijiri medicale la momentul potrivit care vor fi plătite de către Compania de Asigurări. Valoarea compensării poate fi revizuita daca deteriorarea sanatatii s-a produs din cauza mea.
10. Sunt de acord ca probele de sânge recoltate in timpul studiului sa fie pastrate la Centrul Clinic sau la laboratorul analitic in condiţii corespunzătoare.
11. Sunt de acord cu accesul direct la datele mele personale si înregistrările medicale, si cu transmiterea doar a înregistrărilor mele medicale către Sponsor sau reprezentanţii acestuia. Autorităţilor de sanatate relevante si Comisiei Naţionale de Bioetica. Nu renunţ la nici un drept legal ca rezultat al semnării acestui Formular de Consimtamant Informat.
12. Am inteles faptul ca daca informaţii noi care pot fi relevante pentru consimţământul meu pentru a continua participarea in studiu devin disponibile, voi fi informat. Mi s-a oferit posibilitatea de a fi informat asupra rezultatelor generale ale studiului.

Confirm ca am întrebat si voluntarul a confirmat ca el/ea a primit informaţii complete privind natura, scopul si posibilele riscuri ale studiului clinic de mai sus: " '

Semnat de Dr.: _____/_____ Data:_____
(numele) (semnatura) (ziua, luna, anul)

Am primit explicaţii, am citit si am inteles:

Semnat de voluntar:_____ Data: _____
(ziua, luna, anul)

. Acordul pacientului
pentru transfuzia singelui gi componentelor de singe de la donator
1. Mie (numele gi prenumele pacientului sau a reprezentantului Iui Iegitim)
mi s-a explicat starea sinltIlii mele gi prezen{a indica{iilor pentru
(componentelor de singe).
4
2. Prin prezenta, eu ii incredin{ez medicului
transfuzia singelui de la clonator
(ulterior Nlledic) gi asistenfilor lui dreptul si efectueze urmitoarele investigafii:
3. Confinutul acfiunilor medicale indicate mai sus, riscul posibil, complica{iile posibile, de asemenea qi alternativele metbdei propuse imi sunt eunoscute.
Mi s-a comunicat c[singele de la donator se examineazi cu utilizarea test-sistemelor certificate imunof'ermentfltive la anticorpi confra vimsului hepatitei C, anticorpi contra virusurilor HIV/SIDA 1/2, anticorpi contra agentului care provoaci sifilisul, antigenului superficial alhepatitei B (HBs Ag), la alaninaminotransferazd, grupa de singe ABO gi Rhezus antigeni. Insi dupl transfuzia singelui gi a componentelor de singe de la donator, in organismul meupot sd se dezvolte reacfii sau complicafii, in pofida controlului.minufios la selectarea donatorilor,examinirii de laborator a singelui lor gi toate mdsurile posibile de profilaxie, previzutede documentele in vigoare.
Din rindul reactiilqr qi complicafiitor pot si fie hemolitice, nehemolitice, febrile, urticirie, anafilactice, insuficienfi pulmonard acuti, complica{ii aloimune, trombocitorefractare, boala
„transplant
contra
gazdei" gi imunomodulare. Din reacfiile gi complicafiile neimune se pot dezvolta complicafii hemolitice, septice, circulatorii, metabolice, embolice, suprainc[rcarea metabolici cu fier, infec{ioase, inclusiv transmiterea virusurilor hepatitei, HIV/SIDA etc).
4.Eu am avut posibilitatea sd pun dif'erite intrebiri gi Ia toate intrebdrile am primit rispunsuri complete.
5. Eu confirm ci i-am comunicat medicului tot c-e fine de sinitatea mea, l-am informat despre starea fizicd
;i
psihologici.
5. Eu infeleg, cI pe parcursul indeplinirii acfiunilor medicale indicate mai sus pot apdrea imprejuriri neaqteptate, care pot modifica caracterul acfiunilor acordate sau care necesitl examiniri suplimentare, manipulafii, proceduri neindicate in punctul 2. Eu ii increclinfez medicului gi asisteirfilor lui si ia deciziile :espective in conformitate cu judecata lor profesionallgi sI efectueze orice acfiuni medicale, pe care le va :onsidera necesare pentru ameliorarea stlrii mele.
i. Transfuzia singelui de la donator (a componentelor ei) se poate asocia cu utilizarea substituentelor de ;inge, a eritropoietinei
Ei
a preparatelor de fier gi a altor preparate.
{id
Nafional in Transfuziologie
lrEu confirm prin semnltura mea,acordul la recoltarea pretransfuzionalS analizei HMSIDA gi ci am ftit qi infeleg tot ce este expus mai sus. Medicul arlspuns la toate intreb[rile mele. (Numele,prenumele racientului gi reprezentantului legitim pentru persoanele mai tinere de 15ani)
Semn[tura medicului (numele, prenumele)
lu refuz transfuzia singelui de la donator gi/sau a componentelor sanguine prin prezenfa'indicafiilor, :eea ce confirm prin semnitura mea. Mie mi s-au explicat posibilele'consecinfe ale refuzLlui.
iemnltura pacientului (sau a reprezentantului legitim pentru persoanele mai tinere de 15 ani) (Numele gi rrenumele)
Semqitura medicului (numele, prenumele)

Anexa 2

La ord. nr.___ din _____

Regulamentul privind asigurarea securităţii datelor cu caracter personal (medical), prelucrare acestora în mod manual(pe suport de hârtie) în IMSP "Spitalul Clinic al Ministerului Sănătății"

1.Prevederi generale

1.1. Fisele medicale de ambulatoriu (forma 025/e), a copiilor (form. 112/e) a gravidelor (form. 111/e) a tuturor pacienţilor înregistraţi în IMSP SCMS precum si alte formulare si registre se consideră purtătoare de date cu caracter personal.

1.2. Aceste fişe medicale a fi păstrate de lucrătorii medicali în birouri si spatii special destinate (registraturi, birouri a medicilor de familie, asistentelor medicale, cabinete ginecologice, laboratoare)

1.3. Fişele medicale de ambulatoriu (forma 025/e), (form. 112/e),a tuturor pacienţilor înregistraţi în IMSP SCMS sunt păstrate în registratura instituției. Păstrarea fişelor pe perioada concediului medical, copiilor până la un an de viaţă si femeilor însărcinate se păstrează în cab. medicilor de familie.

1.4. Transmiterea fişelor medicale din registratură în cabinetele medicilor de familie se asigură numai de registrator si asistentele medicilor de familie.

1.5. Nu se permite eliberarea fişelor medicale în original pacienţilor (părinţilor copiilor).

1.6. Medicii vor efectua înscrierile în fişele medicale noi în cazurile când pacienţii refuză să reîntoarcă în instituţie fişele medicale păstrate la domiciliu.

1.7. Familiarizarea pacientului (părintelui copilului) cu propriile date cu caracter personal se execută în corespundere cu actele normative în vigoare, la cererea lui şi poate fi realizată prin eliberarea fişei medicale în original pacientului.

1.8. În cazurile prevăzute de actele normative în vigoare fişele medicale pot fie eliberate (scoase din instituţie) numai prin înregistrarea acestui fapt în registrul special din registratura sau registru din arhivă.

1.9. În scopul evitării divulgării datelor cu caracter personal se cere obligatoriu stabilirea identităţii persoanei care recepţionează formularele medicale prevăzute pentru eliberarea pacientului prin verificarea buletinului de identitate.

1.10. Nu se permite discuţie la telefon referitor la date cu caracter personal, cu excepţia situaţiilor când cert este cunoscută identitatea persoanei.

2. Consimţământ pentru prelucrarea datelor cu caracter personal

2.1. Practic, acordarea asistenţei medicale, la etapa de programare si documentare prevede prelucrarea datelor cu caracter personal.

2.2. Datele cu caracter personal a beneficiarilor de servicii prestate în IMSP SCMS pot fi prelucrate numai cu consinţământul lor.

2.3. Consimţământul pentru prelucrarea datelor se obţine prin completarea formularului special(Model)

2.4. Prelucrarea datelor cu caracter personal referitor la pacient se efectuează cu consimţământul lui, cu excepţia cazurilor, prevăzute de Lege. Modelul c consimţământului este ataşat la fişa medicală a pacientului la prima filă. Obţinerea consimţământului este necesară la prima adresare, la fiecare adresare se verifică existenţa consimţământului. în cazul dispariţiei acestui consimţământ necesită restabilire. Refuzul pacientului de aşi exprima consimţământul pentru prelucrarea datelor personale face imposibilă acordarea serviciilor medicale(cu excepţia celei urgente).

2.5. Familiarizarea beneficiarilor de servicii, inclusiv părinţilor copiilor, referitor la scopul si efectele consimţământului se efectuează de asistentele medicului de familie, medicii de familie, asistentele medicilor specialişti.

2.6. Medicii, asistentele medicului de familie, asistentele medicilor specialişti, **laborant, alt personal**

a)Asigura înregistrarea deplină si corectă a datelor cu caracter personal despre starea sănătăţii, obţinute în urma consultului si examinării pacientului sau probelor în documentaţia medicală,
b)Asigura prin intermediul asistentelor medicale din cabinetele medicale reîntoarcerea în registratură a fişelor medicale de ambulatoriu, după consultul sau examenul medical al pacientului.

2.7.Asistentele medicale

a)Pregătesc fişele medicale pentru consultul clinic sau diagnostic al pacientului.
b)Reîntorc fişele medicale în registraturi sau alte birouri medicale
c)Poartă răspundere personală pentru executarea prevederilor Legislaţiei şi actelor normative în vigoare referitor la prelucrarea si asigurarea securităţii datelor cu caracter personal, în secţiile subordonate.

2.8.Registratorul medical

a)Identifică locul de păstrare, la necesitate formează sau selectează fişele medicale pentru consult la medicii de familie sau specialişti.
b) Recepţionează fişele medicale reîntoarse şi distribuie conform locului păstrării.

2.9.Asistenta superioară

a)Monitorizează si informează imediat administraţia instituţiei despre abaterile de la cerinţele prevăzute în prelucrarea si asigurarea securităţii datelor cu caracter personal cu propuneri şi întreprinderea măsurilor ce se impun.
b)Asigură prin intermediul personalului din registratură, asistentelor medicale a medicilor de familie selectarea şi în caz de necesitate perfectarea noilor fişe medicale de ambulatoriu pentru pacienţii programaţi la medicii de familie cu notificarea în registrul de evidenţă a fişelor.

Anexa 3

La ord. nr.___ din _____

Regulamentul cu privire la protecţia datelor cu caracter personal, prelucrare cu utilizarea tehnologiilor informaţionale în IMSP ”Spitalul Clinic al Ministerului Sănătății”

1.Noţiuni generale

Prezentul document este elaborat în baza Legii privind protecţia datelor cu caracter personal nr.13 din 08.07.2011, Hotărârii de Guvern nr.1123 din 14.12.2010 privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal şi ordinul IMSP SCMS Nr. ____ din _____

Scopul - Regulamentului cu privire la protecţia datelor cu caracter personal, prelucrare cu utilizarea tehnologiilor informaţionale în IMSP SCMS este protejarea şi minimalizarea distrugerii datelor din cauza unor factori de pericol externi sau interni, întâmplători sau premeditate şi stabilirea măsurilor tehnice şi organizatorice necesare pentru asigurarea securităţii, confidenţialităţii şi integrităţii datelor cu caracter personal.

Date cu caracter personal - orice informaţie referitoare la o persoană fizică identificată sau identificabilă. Persoana identificabilă este persoana ce poate fi identificată direct sau indirect, prin referirea la un număr de identificare sau la unul sau mai multe documente specific identităţii sale fizice, fiziologice, psihice, economice, culturale sau sociale.

2. Date cu caracter personal se împart în două categorii: obişnuite şi speciale

2.1. Categoria obişnuită(Nivel de securitate nr.1) o constituie informaţia ce dezvăluie

1. Numele,Prenumele	2.Sexul
3.Data şi locul naşterii	4.Cetăţenia
5.IDNP	6.Imaginea
7.Vocea	8.Situaţia familiară
9.Situaţia militară	10.Datele de trafic
11.Porecla- Pseudonimul	12.Datele personale ale membrilor familiei
13.Datele din permisul de conducere	14. Datele din certificatul de înmatriculare
15.Situaţia economică şi financiară	16.Datele privind bunurile deţinute
17.Datele bancare	18.Semnătura
19. Datele din actele de stare civilă	20. Numărul dosarului de pensie
21.Codul de asigurări social PASS	22.Codul asigurări medicale CNAM
23.Numărul de tel/fax	24. Numărul de tel. mobil
25.Adresa, domiciliu/reşedinţa	26.Adresa email
27.Datele genetice	28. Datele biometrice și antroprometrice
29. Datele dactiloscopice	30.Profesia, locul de muncă
31.Formarea profesională, diplomă, studii	32.Obişnuinţele, preferinăele, comportamentul
33.Caracteristicele fizice	

2.2Categoria specială (Nivel de securitate nr.2) a datelor cu caracter personal o constituie informaţia care dezvăluie originea rasială sau etnică, convingerile politice, religioase apartenenţa socială, datele privind stare de sănătate sau viaţă intimă, condamnările penale, sancţiuni contravenţionale a persoanei fizice.

Colaboratorii secţiei tehnologii informaţionale colectează, deţin şi prelucrează categoria obişnuită şi categoria specială de date cu caracter personal, nivelul de securitate N-1,N-2, conform Hotărârii Guvernului nr.1123 din 14.12. 2010 privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal.

3.Date cu caracter personal.

Date cu caracter personal ce se prelucrează în SIA sunt următoarele:

1 Numele,Prenumele	2. Sexul
3.Data şi locul naşterii	4. Adresa, domiciliu, reşedinţa
5.IDNP	6.Date privind date de sănătate

Această listă este determinată conform cerinţelor faţă de asigurarea securităţii datelor cu caracter personal şi prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal aprobate prin Hotărârea Guvernului nr.1123 din 14.12.2010.
Prelucrarea datelor cu caracter personal se efectuează numai cu consimţământul pacientului exprimat în scris. În cazul incapacităţii de exerciţiu sau al capacităţii de exerciţiu limitate, consimţământul privind prelucrarea datelor cu caracter personal se acordă în formă scrisă de către reprezentantul lui legal. Modalitatea obţinerii consimţământului este determinată prin alte regulamente, aprobate la nivel de instituţie.

4.Sistemul Informaţional.
Sistemul Informaţional de prelucrare adatelor cu caracter personal din IMSP SCMS este alcătuit din următoarele elemente (mijloace tehnice şi soft)

1. Staţie de lucru
2. Servere
3. Sisteme de dirijare a bazelor de date
4. Hotarul reţelei locale–incintele blocurilor A,B,C,D din IMSP SCMS.
5. Canalele telecomunicaţii de uz naţional şi internaţional

La nivelul fiecărui element ale structurii SIA privitor la identificarea şi autentificarea mijloacelor tehnice, utilizatorilor li fluxurilor de date, sunt implementate şi practicate diferite politici, realizarea cărora este posibilă în urma utilizării sistemelor operaţionale şi aplicaţiilor de gestiune a bazelor de date.
Mijloacele tehnice de prelucrare a datelor cu caracter personal, informaţia care conţine date cu caracter personal sunt scoase din perimetrul de securitate doar în temeiul unei permisiuni scrise a conducerii IMSP SCMS.

5. Identificarea şi autentificarea utilizatorului SIA de date cu caracter personal

5.1.Identificarea şi autentificarea utilizatorului.
Toţi utilizatorii(inclusiv personalul care sigură susţinerea tehnică, administratorii de reţea, progamatorii şi administratorii bazelor de date) au un identificator personal (ID – utilizatorului), care nu conţine informaţie despre nivelul de accesibilitate al utilizatorului.
Pentru confirmarea ID-ului utilizatorului sunt utilizate parole irepetabile cu lungimea de nu mai puţin de 8 caractere ce conţin litere din ambele registre, cifre şi alte semne simbolice.
În cazul când contractul de muncă – raporturile de serviciu ale utilatorului sunt încetate, suspendate sau modificate şi noile sarcini nu necesită accesul la date cu caracter personal ori drepturile de acces ale utilizatorului sunt modificate, ori utilizatorul a abuzat de codurile primite în scopul comiterii unei fapte prejudiciabile, a absentat o perioadă îndelungată codurile de identificare şi autentificare se revocă sau se suspendă primirea informaţiei respective de la serviciul resurse umane.

5.2Administrarea identificatorilor utilizatorilor
Administrarea identificatorilor utilizatorilor include:

1. Identificarea univocă al fiecărui utilizator

2. Verificarea autenticităţii fiecărui utilizator
3. Obţinerea autorizaţiei de la persoana responsabilă (serviciul resurse umane) pentru eliberarea ID-lui utilizatorului
4. Garantarea factorului că ID-ul utilizatorului este eliberat unei persoane determinate concret.
5. Dezactivarea contului de utilizator după o perioadă inactivă stabilită în timp (inacţiunea în perioada de maxim două luni).
6. Executarea copiilor de arhivă

6. Utilizarea probelor în procesul asigurării securităţii informaţionale.

6.1. Regulile de asigurare a securităţii informaţionale.

Regulile de asigurare a securităţii informaţionale în cazul alegerii şi folosirii parolei include:

1. Păstrarea confidenţialităţii parolelor
2. Interzicerea înscrierii parolelor pe suport de hîrtie, în cazul în care nu se asigură securitatea păstrării acestuia
3. Modificarea parolelor de fiecare dată când sunt prezente indiciile eventualei compromiteri a sistemului sau parolei.
4. Alegerea parolelor calitative cu a mărime de minim 8 simboluri, care nu sunt legate de informaţia cu caracter personal a utilizatorului, nu conţin simboluri identice consecutive şi nu sunt compuse integral din grupul de cifre sau litere
5. Modificarea parolelor peste interval de maxim 3 luni
6. Dezactivarea procesului automatizat de înregistrare(cu folosirea parolelor salvate)

6.2Administrarea parolelor utilizatorilor.

Este asigurată posibilitatea utilizatorilor de a alege şi schimba parolele individuale.
Este asigurată blocarea accesului după trei tentative greşite şi autentificate.
La momentul introducerii, parolele nu se reflectă în clar pe monitor.
Parolele se păstrează în formă cifrată, utilizându-se algoritmul criptografic unilateral.

6.3.Informaţii de avertizare.

Înainte de acordarea accesului în sistem ,utilizatorii sunt informaţi despre faptul că folosirea sistemelor informaţionale de date cu caracter personal este controlată şi că utilizarea neautorizată a acestora se urmăreşte în conformitate cu legislaţia.

6.4. Blocarea sesiunii de lucru.

Sesiunea se lucru în SIA destinat prelucrării datelor cu caracter personal se blochează la solicitarea utilizatorului sau automat după maximum 15 min. de perioadă inactivă a utilizatorului), fapt ce face imposibil accesul de mai departe până în momentul când utilizatorul nu deblochează sesiunea de lucru prin metoda trecerii repetate a procedurilor de identificare şi autentificare

6.5. Accesul la distanţă.

Toate metodele de acces de la distanţă la SI de date cu caracter personal sunt securizate (utilizându-se VPN şi criptarea datelor).

7. Asigurarea integrităţii informaţiei care conţine informaţii cu caracter personal şi a tehnologii informaţionale

7.1 Înlăturarea deficienţelor de soft destinate prelucrării datelor cu caracter personal

Se asigură identificarea datelor, înregistrarea şi înlăturarea deficienţelor de soft-turi destinate prelucrării datelor cu caracter personal, inclusiv instalarea corectărilor şi pachetelor de reînnoire a acestor softuri,

7.2 Asigurarea protecţiei contra programelor dăunătoare(viruşilor)

Se asigură protecţia contra infiltrării programelor dăunătoare în sof-uri destinate prelucrării datelor cu caracter personal, măsura ce asigură posibilitatea reînnoirii automate şi la timp a mijloacelor de asigurare a protecţiei contra programelor dăunătoare şi signaturilor de viruşi.

8. Copiile de rezervă şi restabilirea informaţiei care conţine date cu caracter personal.

8.1 Copiile de rezervă a datelor cu caracter personal se creează automat o data pe zi la ora 23.00, sâmbătă spre duminică la ora 01.00 după metoda de încremenare a datelor. Odată pe săptămână inginerul coordonator responsabil de administrarea bazelor de date creează o copie deplină a datelor cu caracter personal cu salvarea pe un suport de date extern. Această copie se păstrează in loc protejat in afara zonei de amplasare a informaţiei si a soft-urilor de bază, in safeu.

8.2 Copiile de siguranţă se păstrează în cutii metalice cu sigiliu aplicat si stocate in afara zonei de amplasare a informaţiei care continue date cu caracter personal sau soft-urile de bază.

Copiile de siguranţă se testează in scopul verificării siguranţei purtătorilor de informaţii şi integrităţii informaţiei care continue date cu caracter personal.

8.3 Procedurile de restabilire a copiilor de siguranţă se actualizează şi se testează cu regularitate ţi se notaează faptul in Registrul de evidență a copiilor, in scopul asigurării eficacității acestora.

9. Controalele de securitate a sistemelor informaționale de date cu caracter personal

Controalele de securitate a sistemelor informaționale de date cu caracter personal se efectuiază cu regularitate, cel puțin o data pe an.

Controalele de securitate sunt actualizate de fiecare dată cînd deținătorii de date cu caracter personal se reorganizează sau își schimbă infrastructura.

Anexa 4

La ord. nr.___ din _____

Regulamentul cu privire la protecţia datelor cu caracter personal În serviciul resurse umane

1.1 Noţiuni generale

Prezentul Regulament este elaborate în baza Legii privind protecţia datelor cu caracter personal nr. 133 din 08.07.2011, Hotărârii Guvernului nr. 1123 din 14.12.2010 privind aprobarea Cerinţelor faţa de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal şi Codului Muncii al Republicii Moldova.

Scopul – stabilirea măsurilor tehnice şi organizatorice necesare pentru asigurarea securităţii, confidenţialităţii şi integrităţii datelor cu caracter personal, prelucrate în secţia resurse umane.

Date cu caracter personal – orice informaţie referitoare la o persoană fizică identificată sau identificabilă. Persoana identificabilă este o persoana care poate fi identificată direct sau indirect, prin referirea la un număr de identificare sau la unul ori mai multe documente specifice identităţii sale fizice, fiziologice, psihice, economice, cultural sau sociale.

2.Datele cu caracter personal se împart în două categorii: obişnuite şi speciale.

2.2 Categoria obişnuită (nivel de securitate N-1) o constituie informaţia care dezvăluie:

1.Numele, prenumele;
2.Sexul
3.Data şi locul naşterii;
4.Cetăţenia;
5.IDNP;
6.Imaginea;
7.Vocea;
8.Situaţia familiară;
9. Situaţia militară;
10.Datele de trafic;
11.Porecla/pseudonimul;
12.Datele personale ale membrilor familiei;
13.Datele din permisul de conducere;
14.Datele din certificatul de înmatriculare;
15.Situaţia economică şi financiară;
16.Datele privind bunurile deţinute;
17. Datele bancare;
18. Semnătura;
19. Datele din actele de stare civilă;
20.Numărul dosarului de pensie;
21.Codul de asigurării sociale (CPAS);
22. Codul de asigurării medicale (CPAM);
23.Numărul de telefon/fax;
24. Numărul de telefon mobil;
25.Adresa (domiciliu/reşedinţa);
26. Adresa e-mail;
27.Datele genetice;
28.Datele biometrice şi antropometrice;
29.Datele dactiloscopice;
30.Profesia şi/sau locul de muncă;
31.Formarea profesională -diplome-studii;
32.Obişnuinţele/ comportamentul;
33.Caracteristicile fizice.

2.1. Categoria specială (nivel de securitate N-2) a datelor cu caracter personal o constituie informaţia care dezvăluie originea rasială sau etnică, convingerile politice, religioasă, apartenenţa social, datele privind starea de sănătate sau viaţa intimă, condamnările penale, sancţiuni contravenţionale ale unei persoane fizice.

Responsabilul resurse umane colectează, deţine şi prelucrează categoria obişnuită şi categoria specială de date cu caracter personal, nivelurile de securitate N-1 şi N-2 conform Hotărârii Guvernului nr. 1123 din 14.12.2010 privind aprobarea Cerinţelor faţa de asigurarea securităţii datelor cu caracter personal.

3.Datele cu caracter personal în serviciul resurse umane sunt:

Orice informaţie referitoare la angajaţi, enumerate în p.2.1. şi p. 2.2. şi reflectată în sistemul informaţional, în dosarul personal, fişa personală MR-2, contractul individual de muncă, acordurile suplimentare la contractual individual de muncă şi diverse Registre specifice serviciului resurse umane.

4. Condiţiile de bază pentru prelucrarea, stocarea şi utilizarea datelor cu caracter personal.

Prelucrarea categoriilor special de date cu caracter personal se efectuează numai cu consimţământul salariatului.

În cazul incapacității de exercițiu sau al capacității de exercițiu limitate, consimțământul privind prelucrarea datelor cu caracter personal se acordă, în formă scrisă, de către reprezentanţii lui legal.

4.1. La prelucrarea categoriilor obișnuite de date cu caracter personal responsabilului resurse umane este obligat să respecte următoarele cerințe:

a) Colectarea şi prelucrarea datelor personale ale salariatului poate fi efectuată exclusiv în scopul angajării, instruirii, avansării în serviciu, atestării, perfecționării, furnizării datelor către Asociațiile medicilor de profil;

b) Toate datele personale urmează a fi preluate numai de la salariat sau din sursa indicată de acesta;

c) Să utilizeze datele cu caracter personal ale salariatului;

d) Să familiarizeze salariații sub semnătură, cu actele angajatorului cu caracter individual şi normative, vizînd modul de prelucrare şi păstrare a datelor cu caracter personal;

e) Să utilizeze date cu caracter personal al salariaților numai în limitele competențelor funcționale doar în timpul orelor de program;

f) Să excludă sau să rectifice, la solicitarea salariatului, datele personale incorecte sau incomplete şi a informațiilor care se păstrează nelegitim;

4.2. Responsabilul resurse umane nu are dreptul:

a) Să obțină şi să prelucreze date referitoare la convingerile politice religioase, la viața privată. În cazurile prevăzute de lege, pot solicita şi prelucra date despre viața privată a salariatului numai cu acordul scris al acestuia;

b) Să obțină şi să prelucreze date privind apartenența salariatului la sindicate, asociații obștești şi religioase, partide şi alte organizații social-politice;

4.3 Transmiterea datelor personale ale salariatului.

La transmiterea datelor personale cu caracter personal a salariaților responsabilul resurse umane trebuie să respecte următoare cerințe:

- Să nu comunice unor terți datele personale ale salariaților fără acordul scris al acestuia, cu excepția cazurilor prevăzute de lege, precum şi în caz de pericol pentru viața sau sănătatea salariatului;
- Să permită accesul la datele personale ale salariatului doar persoanelor împuternicite necesare exercitării unor atribuții de serviciu (directorul, contabilitate, asistentei superioare, comitetului sindical şi altora în conformitate cu legislația în vogoare);
- Să prevină persoanele care în exercițiul funcțiunii solicită şi primesc date cu caracter personal ale salariaților că poartă răspundere în conformitate cu legislația pentru divulgarea lor, luându-se în considerație prejudicial adus prin aceasta salariatului.

4.4. Păstrarea datelor cu caracter personal.

a) De comun cu serviciul TI, să asigure protecția datelor cu caracter personal în procesul exploatării sistemului informațional: prevenirea scurgerii informației, distrugerii, modificării, copierii;

b) Neadmiterea accesului neautorizat la datele cu caracter personal a persoanelor străine;

c) Predarea datelor cu caracter personal în arhiva instituției conform Nomeclatorului aprobat;

d) Distrugerea documentelor care conțin date cu caracter personal conform cerințelor Regulamentului

Comisiei permanente de lucru pentru expertiza arhivei IMSP SCMS;

e) Păstrarea carnetelor de muncă în safeuri metalice şi excluderea eliberării informaţiei din acestea persoanelor terţe;

f) Respectarea confidenţialităţii în procesul executării obligaţiunilor de funcţie conform angajamentului asumat anterior;

g) Furnizarea informaţiei în alte instituţii care conţine date cu caracter personal numai dacă este bază legală;

h) Nu se admite scoaterea documentaţiei care conţine date cu caracter personal din birou, instituţie sau lăsată fără supravegere;

i) Păstrarea confidenţialităţii parolei, schimbarea ei periodică;

j) Furnizarea informaţiei în alte instituţii care conţine date cu caracter personal la solicitările parvenite de peste hotare se efectuează numai cu acceptul Centrului pentru Protecţia Datelor cu Caracter Personal;

k) Informarea imediată a administraţiei despre apariţia unor accidente de securitate;

l) Securitatea biroului:

- safeurile permanent închise

- la finele zilei de muncă se încuie uşile şi ferestrele

- nu se admite accesul persoanelor străine la computer

- respectarea cerinţelor şi asigurarea securităţii contra incendiilor şi altor posibile riscuri.

4.5. Drepturile salariatului privind asigurarea protecţiei datelor sale personale care se păstrează în serviciul resurse umane.

Salariatul are dreptul:

a) De a primi informaţia deplină despre datele sale personale şi modul de prelucrare a acestora;

b) De a avea acces liber şi gratuit la datele sale personale, inclusiv dreptul la o copie de pe orice act juridic care conţine datele personale;

c) De a cere excluderea sau rectificarea datelor personale incorecte sau incomplete, a informaţiilor care se păstrează nelegitim;

d) De a ataca în instanţa de judecată orice acţiuni sau inacţiuni ilegale ale angajatorului admise la obţinerea, păstrarea, prelucrarea şi protecţia datelor personale ale salariatului.

5. Persoană responsabilă de prelucrarea, stocarea şi utilizarea datelor cu caracter personal este responsabilul resurse umane.

6. Responsabilitatea pentru încălcarea normelor privind obţinerea, păstrarea, prelucrarea şi protecţia datelor personale ale salariatului.

Personalul serviciului resurse umane şi alte persoane care în exerciţiul funcţiunii au luat cunoştinţă cu datele cu caracter personal, poartă răspundere, în conformitate cu legislaţia, pentru divulgarea acestor date, luându-se în considerare prejudicial adus aceasta subiectului de date.

Consimţământul

Salariatului privind obţinerea, păstrarea, prelucrarea şi protecţia datelor lui personale.

Elaborat conform art. 5 și art. 6 din

Legea privind protecţia datelor cu caracter personal nr.133 din 08.07.2011.

(se completează de salariat personal)

Eu, subsemnata_____prin prezentul îmi exprim acordul
(Numele, Prenumele)

ca IMSP SCMS să colecteze, să prelucreze, să păstreze şi să furnizeze datele mele personale în limita exercitării atribuţiilor de serviciu de către persoanele împuternicite, precum şi în scopul îndeplinirii unei obligaţii care îi revine operatorului conform legii.

Datele personale ce se referă la mine pot fi folosite exclusive în scopul angajării, instruirii, avansării, atestării, perfecţionării, furnizării datelor către Compania Naţională de Asigurări în Medicină, Agenţia Teritorială de Asigurări în Medicină, Ministerul Sănătăţii, Direcţia Sănătăţii, Centrul Naţional de Management în Sănătate, Asociaţiilor medicilor de profil, precum şi în scopul examinării cererilor depuse de mine în alte instanţe şi a cererilor terţilor care au ca obiect activitatea mea profesională.

Îmi exprim angajamentul de a asigura confidențialitatea informațiilor cu accesibilitate limitată cunoscute de către mine în IMSP SCMS, inclusiv și după încetarea raportului juridic de muncă.

Confirm ca am fost informat de prevederile "Politicii de securitate privind protecția datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale gestionate de si Regulamentele _____ " si ca mi s-a adus la cunostinta drepturile mele prevăzute de art. 12-16 ale Legii 133 privind protecția datelor cu caracter personal (dreptul de acces, de intervenție, de opoziție, precum de a mă adresa în instanța de judecată, în contextul prelucrării efectuate asupra datelor cu caracter personal ce mă vizează) și responsabilitățile mele privind prelucrarea datelor cu caracter personal.

Semnat de mine personal

Data _____ Semnătura_____

Anexa 5

La ord. nr.___ din _____

Regulamentul

privind asigurarea securităţii datelor cu caracter personal a pacientului în cadrul IMSP "Spitalul Clinic al Ministerului Sănătății"

I. Dispoziţii generale

1.1. Regulamentul cu privire la asigurarea securităţii datelor cu caracter personal a pacienţilor în cadrul IMSP SCMS stabileşte securitatea şi responsabilitatea personalului medical care activează în IMSP SCMS ce au acces direct sau indirect la datele cu caracter personal.

1.2. Regulamentul are scopul de a asigura nivelul corespunzător al protecţiei datelor cu caracter personal ale persoanelor ce benificiază de servicii medicale prin aplicarea corespunzătoare a legislaţiei naţionale cu referire la protecţia datelor şi confidenţialitatea comunicării.

1.3. Personalul medical nu vor depăşi limitele stabilite de Politica de securitate a IMSP SCMS precum şi normele legale stabilite prin prevederile Legii nr. 133 din 8 iulie 2011 cu privire la protecţia datelor cu caracter personal şi ale Legii nr. 71 din 22 martie 2007 cu privire la registre.

II. Scopul prelucrării şi nomenclatorul datelor cu caracter personal disponibile

2.1. Scopul prelucrării datelor cu caracter personal în cadrul IMSP SCMS este prestarea servicilor medicale acordate pacienţilor în vederea derulării programelor naţionale de sănătate.

2.2. Toate fişelele medicale de ambulator şi staţionar (F025/e, 112/e, F 111/e, 112/e, 113/e, 003/e) a pacienţilor internaţi în cadrul IMSP , inclusiv alte formulare şi registre 001/e, 002/e, 008/e, 010/e, 015/e ,102/e, 069/e, 035/e, 050/e, 060/e, 092-2/e, 145-1/e, 155-1/e, 250-1/e, 250-2/e, 250-3/e, 250-4/e, 253/e, 256/e, 257/e, 258/e, 259/e, 260/e, 316/e, 336/e, 366/e, fişe de suport pe hîrtie, note informative la cazuri de deces, recenzii, certificate, extrase, trimiteri la învestigaţii care conţin date cu caracter personal- se consideră purtătoare de date cu caracter personal.

2.3. Întru realizarea scopului de prestarea servicilor medicale, medicii şi asistentele medicale a IMSP SCMS sunt în drept de a solicita de la persoana ce se adresează pentru acordarea asistenţei medicale la IMSP SCMS următoarele date:

- Numele , prenumele
- Data, luna şi anul naşterii
- Codul asigurării medicale

- Numărul de telefon, mobil
- Adresa de domiciliu
- Profesia şi /sau locul de muncă
- Semnătura
- IDNP
- Cetăţenia
- Grupa de sînge
- Sexul
- Diagnoza
- Seria şi numărul certificatului de naştere
- Vărsta
- Funcţia
- Locul de trai

III.Măsurile de asigirare întreprinse în vederea protecţie a datelor cu caracter personal a pacientului în cadrul IMSP SCMS .

Întru respectarea confidenţialităţii datelor cu caracter personal, personalul medical vor respecta cu stricteţe următoarele reguli:

2. La completarea fişelor medicale de ambulator şi staţionar (025/e, 111/e, 112/e,113/e, 003/e, etc.), altor formulare de evidenţă sau supraveghere medicală sau epidemiologică să fie consimţământul scris persoanei pentru prelucrarea (colectarea, stocarea, utilizarea şi transmiterea) informaţiei de sănătate.

3. Transmiterea fişelor medicale a pacienţilor din secţia internare în cabinetele medicilor specialişti, şefilor de secţii, cabinetul certificatelor medicale, servicii diagnostice se asigură numai prin personalul medical şi auxiliar autorizat.

4. Toate documentele medicale ce conţin date cu caracter medical şi personal urmează a fi păstrată de lucrătorii medicali/salariaţi în birouri şi spaţii special destinate (registraturi, birouri ale medicilor, asistentelor medicale, cabinete diagnostice, laboratoare, contabilitate, arhivă) în safeuri şi dulapuri metalice care se încuie.

5. Fişele medicale pot fi eliberate (scoase din instituţie) numai în baza cererii scrise a solicitantului cu înregistrarea acestui fapt în registrul special din secretariat sau alt registru prevăzut din arhivă.

Cererea se va întocmi pe numele conducătorului instituţiei medicale şi se va depune la cancelaria instituţiei.

La cererea scrisă va conţine:

1.datele de identificare a solicitantului,

2.date suficiente şi concludente pentru identificarea informaţiei solicitate (date despre aflarea la evidenţa în instituţia dată, date despre perioada

tratamentului ambulatoriu/staţionar efectuat, date despre perioada de efectuare a investigaţilor, motivul intemeiat pentru eliberarea fişei) ,

Cerere va fi însoţită de:

1. Buletinul de identitate a solicitantului,

2. În cazul pacientului care nu a atins virsta de 18 ani se va anexa copia certificatului de naştere sau copia actului oficial ce atestă dreptul de tutore sau curator al pacientului, pacientul care a delegat o altă persoană care să fie informată în locul său, solicitantul va anexa copia de pe procură autentificată notorial.

3. În cazul pacienţilor declaraţi prin hotărîre judecătorească incapabili sau cu capacitate de exerciţiu limitată, solicitantul va anexa la cerere şi copia de pe hotărîrea judecătorească, şi după caz, copia actului oficial, care arestă dreptul de tutore sau curator al pacientului.

6. Accesul direct al pacientului sau al reprezentantului acestuia la informaţia stocată în dosarul lui medical, se va supravghea de către cadru medical sau de persoana supusă declaraţiei de confidenţialitate, care vor supraveghea momentul vizionării dosarului şi vor asigura ca dosarul medical să rămînă în condiţii de siguranţă, fără a face comentarii sau fără a da consultaţii cu privire la cuprinsul dosarului medical.

7. Accesul fizic la informaţiile care conţin date cu caracter personal este interzis şi controlat în scopul înpedicării vizualizării acestora de către alte persoane.

8. Pacienţii trebuie informaţi de către personalul medical atunci cînd sînt prelucrate datele sale cu caracter personal privind starea de sănătate sau dosarele medicale ale acestora prin metoda accesării de către orice terţ sau autoritate publică, precum şi atunci cînd informaţiile sînt sau pot fi transmise unor terţi ori destinatari**.**

9. Utilizatorii datelor cu caracter personal din IMSP vor semna angajament de confidenţialitate (nedevulgarea neautorizată a datelor cu caracter personal şi medical)

10. Nu se admite divulgarea datelor cu caracter personal persoanelor terţe, prin telefon sau prin comunicare directă fără stabilirea identităţii persoanei şi a temeiului legal al solicitării.

11. Nu se admite divulgarea datelor cu caracter personal în discuţii dintre salariaţi cu exepţia cazurilor de necesitate de serviciu.

IV. Consimţămîntul la prelucrarea datelor cu caracter personal.

4 .1. Acordarea asistenţei medicale este iniţiată la etapa de programare a pacientului şi prevede prelucrarea datelor cu caracter personal.

4.2. Datele cu caracter personal a persoanelor ce benificiază de servicii medicale în cadrul IMSP SCMS pot fi prelucrate numai cu consimţămîntul lor.

4.3. Consimţământul pentru prelucrarea datelor se obţine prin completarea unui formular special (anexa nr.1 – *Model: Consimţământul subiectului (pacientului) datelor cu caracter personal privind starea de sănătate*).

4.4.Modelul consimţământului este ataşat la fişa medicală a pacientului. Obţinerea consimţământului este necesară la prima adresare în IMSP SCMS Ulterior, la fiecare adresare, pînă la acordarea asistenţei medicale programate se verifică existenţa consimţământului. În cazul lipsei/dispariţiei din fişa medicală, acest consimţământ necesită a fi restabilit. Consimţământul se înregistrează prin consemnarea unui formular special, modelul căruia este elaborat şi aprobat de administraţie. Refuzul pacientului de aşi exprima consimţământul pentru prelucrarea datelor personale face imposibilă acordarea serviciilor medicale (cu excepţia celor de urgenţă).

4.5 Familiarizarea beneficiarilor de servicii, inclusiv părinţilor copiilor, referitor la scopul şi efectele consimţământului se efectuează de către asistentele medicale, medicii specialişti.

V. Responsabilităţile şi obligaţiunilr personalului medical la prelucrarea datelor cu caracter personal a pacientului ce benifiaciază de servicii medicale în cadrul IMSP SCMS .

5.1. să aducă la cunoştinţa pacientului scopul prelucrării datelor cu caracter personal - prestarea servicilor medicale
5.2. să aducă la cunoştinţă pacientului despre drepturile acestora la informare, de acces, la intervenţie asupra datelor, la opozuţie, de a nu fi supus unei decizii individuale, acces la justiţie.
5.3. să ceară consimţământul pacientului înainte de a utiliza datele lui cu caracter personal.
5.4. să aducă la cunoştinţa personelor care doresc să benificieze de servicile acordate de instituţie că sunt obligaţi să furnizeze datele cu caracter personal fiind necesare în realizarea scopului de acordarea servicilor medicale şi în caz de refuz determină imposibilitatea de a benificia de servicii medicale oferite de instituţie.
5.5. să explice semnificaţiile transmiterii/acordării accesului/utilizării sau a netransmiterii/acordării accesului/utilizării informaţiilor privind starea lor de sănătate.
5.6. să fie conştienţi de problemele legate de aspectul confidenţialităţii datelor cu caracter personal şi medical .
5.7. să ceară pacienţilor să indice persoana de contact (părinte, soţ/soţie, rudă, prieten) care ar putea lua decizii cu privire la îngrijirea lor, în cazul incapacităţii lor, explicîndu-i-se pacientului că persoanei de contact i se va comunica un volum limitat de date cu caracter personal, în condiţiile în care pacientul acceptă această regulă.

5.8. Medicii care sunt invitaţi pentru consultul pacienţilor în secţia internare sunt obligaţi să nu efectueze examinarea pacientului în prezenţa terţelor persoane.

5.9. să acorde o atenţie sporită la obligaţia de asigurare a regimului de confidenţialitate înainte de a fi transmis dosarul, precum şi să ofere persoanei care accesează datele cu caracter personal privind starea de sănătate, informaţia despre necesitatea asigurării ulterioare de către aceasta a confidenţialităţii datelor

5.10. să verifice dacă pacienţii au neclarităţi sau întrebări legate de modul în care informaţiile cu privire la sănătatea lor sînt utilizate sau transmise;

5.11. să respecte dreptul pacienţilor la acces la dosarele lor medicale;

5.12. să comunice eficient cu pacienţii pentru ai ajuta să înţeleagă importanţa transmiterii informaţiei cu privire la sănătatea lor;

5.13. trebuie să fie examinată minuţios fiecare situaţie, evitîndu-se admiterea încălcărilor ce pot genera nerespectarea regimului de confidenţialitate

5.14. Deciziile de a dezvălui datele cu caracter personal şi justificarea scopului legal pentru transmiterea acestora trebuie menţionate în fişa medicală a pacientului.

VI. DISPOZIŢII FINALE

6.1. Prezentul Regulament întră în vigoare din data aprobării prin ordinul IMSP SCMS.

6.2. Modificarea şi completarea Regulamentului în cauză se efectuează în corespundere cu actele normative în vigoare.

Anexa 6

La ord. nr.___ din _____

REGULAMENT
cu privire la asigurarea securităţii datelor cu caracter personal pentru Sistemul Informaţional de Evidenţă a Pacienţilor din Staţionar în cadrul IMSP "Spitalul Clinic al Ministerului Sănătății"

I. Dispoziţii generale

1. Regulamentul la asigurarea securităţii datelor cu caracter personal în Sistemul Informaţional de Evidenţă a Pacienţilor din Staţionar în cadrul instituţiei medico-sanitare publice "Spitalul Clinic al Ministerului Sănătății" (în continuare IMSP SCMS) stabileşte responsabilităţile persoanelor din subdiviziunile structurale ale IMSP SCMS ce au acces la securitatea datelor cu caracter personal în cadrul aplicaţiei Pacienţilor din Staţionar(PS).

2. Persoanele din subdiviziunile structurale ale IMSP SCMS ce au acces la securitatea datelor cu caracter personal în cadrul aplicaţiei PS nu vor depăşi limitele stabilite de Politica de securitate a IMSP SCMS, precum şi normele legale stabilite prin Hotărîrea Guvernului nr. 1123 din 14.12.2010 privind aprobarea cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor de date cu caracter personal şi Legii nr.133 din 08 iulie 2011 privind protecţia datelor cu caracter personal.

3. Regulile obligatorii ce se vor aplica în toate subdiviziunile structurale din IMSP SCMS care au acces la sistemul de datele cu caracter personal - aplicaţia PS pentru asigurarea:

a) controlului strict asupra accesului la informaţie;
b) accesului autorizat al utilizatorului şi prevenirea accesului neautorizat la sistemul informaţional;
c) prevenirii compromiterii sau furtului de informaţii şi a sistemelor de procesare a informaţiilor;
d) prevenirii accesului neautorizat la serviciile de reţea;
e) prevenirii accesului neautorizat la sistemele de operare;
f) prevenirii accesului neautorizat la informaţia deţinută în sistemele de aplicaţii;

II. Organizarea măsurilor de protecţie a datelor cu caracter personal

4. Directorul IMSP SCMS desemnează persoana responsabilă de politica securitaţii în cadrul IMSP SCMS care organizează şi asigura:

procedurii de înregistrare a utilizatorului şi de anulare a înregistrării pentru a garanta şi pentru a revoca accesul de monitorizare a respectării prevederilor politicii datelor cu caracter personal;

managementului de acces a utilizatorilor la activele informaţionale ale instituţiei şi monitorizează procesul de înregistrare a utilizatorilor

revizuirea actelor normative în instituţie nominalizînd prin ordin persoanele care vor accesa, prelucra şi întroduce datele de caracter personal în PS şi responsabilitatea acestora în activitatea desfăşurată;

aprobarea persoanelor cu acces la baza de date cu caracter personal;

securitatea accesului fizic în birourile unde sunt amplasate sistemele informaţionale cu conţinut de date cu caracter personal, fiind permis doar persoanele care au autorizarea necesară;

utilizarea unei parole de acces la sistemul de date cu caracter personal;

prelucrarea datelor cu caracter personal va fi efectuat cu consimţământul necondiţionat al subiectului datelor cu caracter personal PS;

politicii de securitate a datelor cu caracter personal şi revizuirea anuală ca rezultat al modificărilor sau reevaluării componentelor acesteia;

securitatea încăperii de păstrare a informaţiilor ce conţin date cu caracter personal: gratii, lacăt, paza locală.

5. Accesul la PS este efectuat de administratorul aplicaţiei şi asigură că ea este în acord cu sarcinile de serviciu după cum urmează:

a) existenţa evidenţei drepturilor de acces aprobate în aplicaţie;
b) pregătirea personalului vizavi de faptul că acestea au înţeles condiţiile de acces;
c) drepturile de acces sunt consistente cu utilizarea documentelor;
d) accesul este audiabil şi identificabil la nivel de proces;
e) fiecare utilizator are asociat un identificator unic;
f) accesul în baza permisiunilor predefinite este restricţionat.

6. Serviciul Secţiei de Internare (în continuare SI) este responsabil de atribuirea responsabilităţilor pentru implementarea procesului privind eliminarea privilegiilor de acces ale angajaţilor care îşi încheie contractele de muncă; modificarea permisiunilor accesului utilizatorilor ale căror sarcini de serviciu se modifică (în cazul avansării sau regresării în funcţie); privilegiierea de acces pentru angajaţii cu acces, care lipsesc mai mult de 5 zile din instituţie, fiind blocate pînă la clarificarea situaţiei.

7. Managementul asigurării securităţii datelor cu caracter personal în PS va prevedea obligatoriu:

alocarea parolelor individuale care se vor monitoriza printr-un proces cu aplicarea următoarelor reguli pentru utilizatori:

li se va cere să semneze în Registru de acordare a identificatorului personal – parola(codul) utilizatorului pentru acces la sistemele informaţionale de date cu caracter personal şi să păstreze confidenţialitatea parolelor personale şi a parolelor de grup numai între membrii grupului;

revizuirea drepturilor de acces ale utilizatorilor la intervale regulate utilizând un proces formal pentru aceasta.

Proprietarii şi custozii implementează procese formale pentru revizuirea cu regularitate a drepturilor de acces dar care obligatoriu se vor realiza: anual; trimestrial, în cazul utilizatorilor privilegiaţi; la modificarea statutului unui utilizator; la reorganizarea activităţii sau introducerii unor tehnologii noi; la modificarea politicii dc acces.

8. Utilizatorilor li se va furniza accesul doar pentru serviciile care au fost autorizaţi în mod specific să le utilizeze:

persoanele responsabile activează doar serviciile de reţea necesare desfăşurării activităţilor subdiviziunii. Toate celelalte servicii de reţea sunt oprite.

9. Identificarea echipamentelor în reţea, autentificarea conexiunilor se va realiza prin:

protecţia porturilor pentru diagnoză; asigurarea de către persoana responsabilă a controlului accesului la nivel de porturi, servicii şi sisteme pentru diagnoză, întreţinere sau monitorizare;

10. Protecţia porturilor de configurare (accesul fizic şi logic la porturile de configurare) se vor efectua în mod sigur verificat:

controlul conexiunilor logice şi fizice se va restricţiona de persoana responsabilă, restricţionînd abilitatea utilizatorilor de a se conecta fizic şi logic la reţea.

Tehnicile de restricţionare vor include:

protecţia fizică a cablurilor; inspecţia fizică a punctelor de conectare din zonele publice;

condiţii de separate în interiorul reţelei se va lua în considerare introducerea controlului în cadrul reţelei, pentru a separa în grupuri serviciile informatice, utilizatorii şi sistemele informatice.

11. Controlul conectării la reţea se va realiza prin capacitatea utilizatorilor de a restricţiona în conformitate cu politica de control, iar conectarea la reţea se va efectua numai prin accesul şi în corespundere cu cerinţele aplicaţiei. Restricţiile aplicate sunt bazate pe politica de acces şi pe cerinţele aplicaţiilor activităţilor instituţiei şi sunt menţinute şi actualizate corespunzător. Aplicaţiile asupra cărora trebuie introduse restricţii sunt: poşta electronică; transfer unidirecţional de fişiere; transfer bidirecţional de fişiere; accesul interactiv.

12. Controlul de rutare în reţea se va realiza prin măsuri de securitate de rutare pentru reţele pentru a se asigura că conexiunile de control al accesului pentru aplicaţiile afacerii computerului şi fluxurile de informaţii nu încalcă politica.

13. Controlul accesului la sistem se realizează prin proceduri de autentificare asigurate prin acces la sistemele de operare în mod controlat, printr-o procedură sigură de conectare.

14. Accesul la sistemul informaţional este permis doar utilizatorilor şi proceselor autorizate. Persoanele responsabile se asigura că procesul de login al angajaţilor reduce oportunitatea accesului neautorizat. Aceasta va include obligatoriu: neafişarea informaţiilor despre sistem; afişarea unui mesaj de atenţionare înaintea furnizării credenţialelor de autentificare; neafişarea parolelor în clar.

Identificarea şi autentificarea utilizatorului se va realiza prin emiterea unui identificator unic (ID-ul utilizatorului) numai pentru uz propriu.

15. Se vor respecta următoarele reguli pentru stabilirea parolelor utilizatorilor: folosirea identificatorilor şi parolelor individuale; schimbarea parolelor după primul login; folosirea parolelor complexe; prevenirea reutilizării parolelor; schimbarea parolelor cu regularitate.

16. Pentru a furniza o securitate sporită cu grad ridicat de risc se vor utiliza restricţii cu privire la limitarea timpului de conectare. Restricţionarea operării aplicaţiilor va include limitarea accesului în cadrul unui interval de 5 minute.

17. Accesul la informaţii şi la funcţiile sistemului de aplicaţii de către utilizatori şi personalul de suport se va restricţiona în conformitate cu politica de control al accesului.

18. Utilizatorii de informaţii vor respecta bunele practici de securitate în selecţia şi utilizarea parolelor, anume:

la selectarea parolelor utilizatorii obligatoriu vor asigura: stabilirea parolelor complexe dar uşor de memorizat; neutilizarea aceeaşi parole pentru mai multe conturi de acces; necrearea parolelor bazate pe ceea, ce ar putea fi uşor de dedus sau obţinut din date personale, de exemplu nume, numere de telefon, date de naştere, etc., sau cu caractere identice consecutive, sau caractere exclusiv numerice sau exclusiv alfabetice.

la modificarea parolelor vor ţine cont de următoarele reguli: se va realiza la un interval specificat prin politica de securitate a parolelor; imediat după instalarea unui echipament; imediat ce un cont a fost compromis.

la prezenţa conturilor privilegiate adminstrative utilizatorii stabilesc parole de minimum 8 caractere şi le modifică pînă la maximum 90 de zile.

în protecţia şi utilizarea parolelor strict se va respecta: nedivulgarea parolei altor persoane; nedivulgarea în momentul introducerii parolei; scrierea pe orice tip de suport a parolei.

19 Utilizatorii trebuie să se asigure că echipamentul lăsat nesupravegheat este protejat în mod corespunzător şi sunt responsabili de:

securizarea locului de muncă chiar şi în situaţia în care nu sunt supervizaţi de o persoană autorizată. Securitatea locului de muncă vizează: curăţenia la locul de muncă; securitatea documentelor şi a dispozitivelor de stocare portabile; securitatea mesajelor electronice; blocarea staţiei de lucru în perioadele de inactivitate(pentru sistema de operare Windows formînd combinaţia de butoane „iconiţa windows + L”; încuierea uşilor; verificarea listingurilor imprimantelor.

comportamentul utilizatorului la locul de muncă reduce probabilitatea vizualizării neautorizate a informaţiilor, accesul sau divulgarea acestora. Comportamentul adecvat include: asigurarea că informaţiile senzitive sunt protejate contra vizualizării de către persoanele aflate în tranzit prin zona de lucru; minimizarea ecranelor calculatoarelor persoanele când sunt persoane în tranzit prin zona de lucru; protejarea documentelor de pe birouri.

III. DISPOZIŢII FINALE

20.Prezentul Regulament întră în vigoare din data aprobării prin ordinul IMSP SCMS.

21.Modificarea şi completarea Regulamentului în cauză se efectuează în corespundere cu actele normative în vigoare.

Anexa 7

La ord. nr.___ din _____

REGULAMENTUL PRIVIND SUPRAVEGHEREA PRIN MIJLOACE VIDEO ÎN CADRUL IMSP ”SCMS”

1. Dispoziții generale

În contextul actual securitatea obiectivelor nu poate fi asigurată fără o supraveghere video eficientă, care să permită, atît monitorizarea în timp real a evenimentelor şi persoanelor suspecte, cît şi înregistrarea imaginilor video.

Aceste sisteme de supraveghere video se adresează, în principal, spațiilor în care se desfășoară activități de vînzare, spații comerciale dar și birourilor de acces public.

Totodată utilizarea unui astfel de sistem include anumite responsabilități și garanții din partea proprietarului de sistem, referitor la prelucrarea și protecția datelor cu caracter personal ce se înregistrează în sistem, atribuții și reglementări descrise în legea nr. 133 din 18.07.2011 privind protecția datelor cu caracter personal.

Din acest motiv este necesară stabilirea unui regulament de securitate privind supravegherea prin mijloace video şi prelucrarea datelor cu caracter personal preluate şi înregistrate în sistemul de monitorizare prin înregistrare video.

2. Regulamentul privind supravegherea prin mijloace video în cadrul IMSP ”SCMS” are drept scop:

- Stabilirea unui set unitar de reguli care reglementează implementarea şi utilizarea sistemului de supraveghere video, în scopul asigurării securităţii persoanelor şi bunurilor, pazei şi protecţiei bunurilor, imobilelor, valorilor şi a materialelor cu regim special, respectînd în acelaşi timp obligaţiile ce revin entității, în calitate de operator de date, conform Legii nr. 133 din 18.07.2011 şi măsurile de securitate adoptate pentru protecţia datelor cu caracter personal, protejarea vieţii private, a intereselor legitime şi garantarea drepturilor fundamentale ale persoanelor vizate.
- Stabilirea responsabilităţilor privind administrarea şi exploatarea sistemului de supraveghere prin mijloace video, precum şi cele privind întocmirea, avizarea şi aprobarea documentelor aferente acestor activităţi.
- Scopul utilizării sistemului video este de a asigura buna administrare şi funcţionare a entității, în special în vederea controlului de securitate şi pază. De asemenea, sistemul video este necesar pentru a sprijini politicile de securitate instituite de actele normative care reglementează protecţia datelor cu caracter personal şi contribuie la îndeplinirea atribuţiilor structurii de securitate.
- Prezentul Regulamentul descrie măsurile care necesită a fi luate de IMSP ”SCMS”

pentru a proteja datele cu caracter personal care sînt prelucrate prin metoda supravegherii video, vieții private și alte drepturi fundamentale și interese legitime ale subiecților.

3. Zonele supravegheate

- Camerele de supraveghere video sînt amplasate în locuri vizibile. Orice utilizare ascunsă a acestora este strict interzisă, cu excepția cazurilor expres reglementate de legislație.
- Camerele de supraveghere video sînt amplasate conform anexei nr. 1 al prezentului Regulament.
- Nu sînt monitorizate zonele în care persoanele pot conta, în mod rezonabil, pe intimitate, precum birourile de serviciu și toaletele.

4. Datele cu caracter personal colectate prin intermediul sistemului de supraveghere video

- Sistemul de supraveghere video este dotat cu detector de mișcare. Toate camerele funcționează în regim 24/24 ore și sînt fixate.
- La darea în exploatare a sistemului de supraveghere video, persoana împuternicită v-a primi instructajul referitor la setările sistemului de monitorizare video, respectarea regimului de confidențialitate și dreptul de acces la informația prelucrată în sistemul de evidență.

5. Limitarea scopului

- Sistemul de supraveghere video va fi utilizat numai în scopul în care este notificat, fără a se urmări în special obținerea unor informații pentru anchetele interne sau procedurile disciplinare, cu excepția situațiilor în care se produce un incident de securitate sau se observă un comportament infracțional (în circumstanțe excepționale imaginile pot fi transmise organelor competente în cadrul unor investigații disciplinare sau penale).
- În vederea protejării vieții private a altor subiecți decît cei vizați nemijlocit, sistemul video este dotat cu mecanisme care prevăd estomparea imaginii (în caz de necesitate) pentru a face ca întreaga imagine sau o parte a ei, după caz, să fie anonimizată.
- Persoana responsabilă va gestiona accesul la sistemul de supraveghere video numai cu acordul scris al conducerii IMSP ”SCMS”.

6. Categorii speciale de date cu caracter personal

- Sistemul de monitorizare video al IMSP ”SCMS” nu are ca scop captarea (spre exemplu prin focalizare sau orientare selectivă) sau prelucrarea imaginilor (spre exemplu indexare, creare de profiluri) care constituie categoria specială de date cu caracter personal.

7. Accesul la datele cu caracter personal și dezvăluirea acestora

- Accesul la imaginile video înregistrate în timp real este limitat la un număr redus de angajați ai IMSP ”SCMS” care pot fi identificați individual, în conformitate cu lista aprobată de către conducerea entității.
- Accesul la imaginile video şi/ sau la arhiva în care sînt stocate imaginile înregistrate este permis numai persoanei responsabile în conformitate cu Politica de securitate a IMSP ”SCMS” și numai cu acordul scris al conducerii.
- Vizualizarea şi/sau efectuarea copiilor din fișierele temporare în care sînt stocate imaginile video, este permis numai cu acordul scris al conducerii.
- În cazul solicitării de către organele de drept ale Republicii Moldova, care își exercită atribuțiile conform legii, a unor copii din fișierele temporare în care sînt stocate imaginile video, este permis numai cu acordul scris al conducerii IMSP ”SCMS”.

8. Protecția sistemului informațional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video

În vederea securizării sistemului informațional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video, se aplică următoarele măsuri tehnice şi organizatorice:

- sistemul informațional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video se păstrează în camera special amenajată;
- responsabilul de protecţie a datelor cu caracter personal și responsabilii de securitate din cadrul entității vor fi consultați înainte de achiziţionarea sau instalarea oricărui nou sistem de supraveghere.
- toate sistemele trebuie să corespundă cerințelor de securitate descrise în legislație (HG nr. 1123 privind aprobarea cerințelor față de asigurarea securității datelor cu caracter personal).
- accesul fizic la sistemul informațional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video are numai persoana responsabilă desemnată şi conducerea IMSP ”SCMS”;
- accesul la înregistrările video prelucrate este restricționat prin introducerea unui șir de parole;
- în cazul deconectării energiei electrice, sistemul informațional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video este dotat cu sursă

autonomă de alimentare cu energie electrică (UPS);

- sistemul informațional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video este dotat cu firewall care asigură protecția în rețea;
- Echipamentele sînt astfel instalate încît să se afle sub supraveghere doar acele spaţii identificate în analiza de risc ca avînd nevoie de protecţie suplimentară.
- Utilizatorii sistemului de supraveghere video sunt instruiţi să nu monitorizeze astfel de zone.
- IMSP ”SCMS” actualizează în permanență listă persoanelor care au acces la sistemul informațional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video, care descrie în detaliu drepturile de acces ale acestora.

9. Control Acces

- Imaginile captate de sistemul de supraveghere video sînt vizualizate în timp real pe monitoarele din camera de control acces, care reprezintă o încăpere securizată, iar monitoarele nu pot fi văzute din exterior.
- Camera de control acces este amplasată în sediul central al entității.
- Accesul neautorizat în Camera de control este interzis. Accesul este strict limitat la angajaţii autorizaţi: personalul cu funcții de asigurare al securității fizice şi control acces, administratorul de sistem, responsabilii cu securitatea informaţiei şi conducerea entității.
- De la caz la caz, se poate acorda accesul în Camera de control şi altor persoane, în afara celor menţionate mai sus, doar pe bază de autorizare din partea responsabilului de securitate din cadrul entității. Aceste persoane nu vor avea acces la datele personale prelucrate în activitatea de supraveghere video, accesul acestora fiind permis strict pentru executarea lucrărilor menționate în autorizarea din partea responsabilului de securitate din cadrul entității.

10. Pentru a proteja securitatea sistemului video şi pentru a spori gradul de protecţie a vieţii private, au fost introduse următoarele măsuri tehnice şi organizatorice:

- limitarea timpului de stocare a materialului filmat, în conformitate cu cerinţele de securitate și legislația în viguare privind conservarea datelor.
- mediile de stocare (serverele pe care se stochează imaginile înregistrate) se află în spaţii securizate și protejate de măsuri de securitate fizică.
- toţi utilizatorii cu drept de acces la sistemul de supraveghere video au semnat acorduri de confidenţialitate, prin care se obligă să respecte prevederile legale în domeniu.
- utilizatorilor se acordă dreptul de acces doar pentru acele resurse care sînt strict necesare pentru îndeplinirea atribuţiilor de serviciu.

- doar administratorii de sistem numiți în acest sens de către operator, și responsabilul de securitate, au dreptul de a accesa fișierele înregistrate în sistem, la cererea conducerii unității.

11. Drepturi de acces

1. Accesul la imaginile stocate şi/sau la arhitectura tehnică a sistemului de supraveghere video este limitat la un număr redus de persoane şi este determinat prin atribuţiile specificate în fişa postului, în care este indicat în ce scop şi ce tip de acces este acordat.
2. IMSP ”SCMS” impune limite stricte în privinţa persoanelor care au dreptul:

- să vizioneze materialul filmat în timp real: imaginile care se derulează în timp real sunt accesibile responsabililor de securitate și agenţilor de pază desemnaţi să desfăşoare activitatea de supraveghere;
- să vizioneze înregistrarea materialului filmat: vizionarea imaginilor înregistrate se va face în cazuri justificate, cum ar fi cazurile prevăzute expres de lege şi incidentele de securitate, de către persoanele special desemnate;
- să copieze, să descarce, să şteargă sau să modifice orice material filmat de sistemul de supraveghere video.

3. Instructaj

- Toţi membrii personalului cu drepturi de acces beneficiază de o instruire iniţială în domeniul protecţiei datelor.
- Această procedură va fi integrată în programul de instruire şi îndrumare, pentru toţi utilizatorii cu drept de acces şi atribuţii în operarea sistemului de supraveghere video.
- Șeful subdiviziunii va asigura că întregul personal din subordine, implicat în operarea sistemului de supraveghere video, este instruit şi informat cu privire la toate aspectele funcţionale, operaţionale şi administrative ale acestei activităţi.

4. Măsuri de păstrare a confidenţialităţii

- Imediat după instructaj, fiecare participant cu drept de acces la sistemul de supraveghere video semnează un acord de confidenţialitate.

12. Dezvăluirea datelor cu caracter personal

- Orice activitate de dezvăluire a datelor personale către terţi va fi documentată şi supusă unei analize riguroase privind pe de-o parte necesitatea comunicării, şi pe de altă parte compatibilitatea dintre scopul în care se face comunicarea şi scopul în care aceste date au fost colectate iniţial pentru prelucrare.
- Orice situaţie de dezvăluire va fi consemnată de administratorul sistemului într-un Registru de evidenţă a cazurilor de dezvăluire.
- IMSP ”SCMS” are obligaţia punerii la dispoziţia organelor judiciare, la solicitarea scrisă a acestora, înregistrările video în care este surprinsă săvîrşirea unor fapte de natură contravenţională/penală.

- Sistemul de supraveghere video nu este utilizat pentru verificarea prezenţei la program sau evaluarea performanţei la locul de muncă.
- În cazuri excepţionale, dar cu respectarea garanţiilor descrise mai sus, se poate acorda acces altor servicii din cadrul entității (Protecție Antiincendiară, Resurse Umane, Riscuri), în cadrul unei anchete disciplinare, de accidentare sau de securitate, cu condiţia ca informaţiile să ajute la investigarea unei infracţiuni, accident de muncă sau a unei abateri disciplinare de natură să prejudicieze drepturile şi libertăţile unei persoane fizice sau juridice.

13. Durata păstrării înregistrărilor video

- Durata păstrării înregistrărilor video este de 30 zile calendaristice, după care acestea se nimicesc automat în ordinea în care au fost înregistrate.
- În cazul producerii unui incident de securitate, durata de păstrare a înregistrărilor video poate depăși limitele admisibile de program, în funcție de timpul necesar investigării suplimentare a incidentului de securitate.

14. Informarea publicului referitor la supravegherea video

Informarea publicului referitor la supravegherea video din cadrul IMSP ”SCMS” se efectuează prin pictograme.

- IMSP ”SCMS” garantează că asigură respectarea drepturilor ce revin persoanelor vizate, în conformitate cu legislația Republicii Moldova. Toate persoanele implicate în activitatea de supraveghere video şi cele responsabile de administrarea imaginilor filmate, vor respecta procedurile și regulamentele de acces la date cu caracter personal ale entității.

15. Informarea persoanelor vizate

- Informarea primară a persoanelor vizate se realizează în mod clar şi permanent, prin intermediul unui semn adecvat, cu vizibilitate suficientă şi localizat în zona supravegheată, astfel încît să semnaleze existenţa camerelor de supraveghere, dar şi pentru a comunica informaţiile esenţiale privind prelucrarea datelor cu caracter personal.
- Persoanele vizate sunt atenţionate asupra existenţei sistemului de supraveghere video şi a proprietarului prin note de informare corespunzătoare, care cuprind scopul prelucrării şi identifică IMSP ”SCMS” ca operator al datelor colectate prin intermediul supravegherii video.

16. Exercitarea drepturilor de acces, intervenţie şi opoziţie

- Pe întreaga perioadă de stocare a datelor cu caracter personal, persoanele vizate au dreptul de acces la datele personale care le privesc deţinute de IMSP ”SCMS”, de a solicita intervenţia (ştergere/actualizare/rectificare/anonimizare) sau de a se opune prelucrărilor, conform legii.
- Orice cerere de a accesa, rectifica, bloca şi/sau şterge date cu caracter personal ca urmare a utilizării camerelor video ar trebui să fie adresată direct IMSP ”SCMS”.
- Răspunsul la solicitarea de acces, intervenţie sau opoziţie se dă în termen de 15 zile calendaristice. Dacă nu se poate respecta acest termen, persoana vizată va fi informată asupra motivului de amînare a răspunsului, de asemenea i se va comunica şi procedura care va urma pentru soluţionarea cererii.
- Dacă există solicitarea expresă a persoanei vizate, se poate acorda dreptul de a vizualiza imaginile înregistrate care o privesc sau i se poate trimite o copie a acestora. Imaginile furnizate vor fi clare, în măsura posibilităţii, cu condiţia de a nu prejudicia drepturile terţilor (persoana vizată va putea vizualiza doar propria imagine, imaginile altor persoanelor care pot apărea în înregistrare vor fi editate astfel încît să nu fie posibilă recunoaşterea/identificarea lor). În cazul unei asemenea solicitări, persoana vizată este obligată:
  - **a.** să se identifice dincolo de orice suspiciune (să prezinte actul de identitate cînd participă la vizionare), să menţioneze data, ora, locaţia şi împrejurările în care a fost înregistrată de camerele de supraveghere.
  - **b.** De asemenea, persoana vizată va prezenta şi o fotografie recentă astfel încît utilizatorii desemnaţi să o poată identifica mai usor în imaginile filmate.
  - **c.** Persoana va putea vizualiza doar propria imagine, imaginile persoanelor care pot apărea în înregistrare vor fi editate astfel încît să nu fie posibilă recunoaşterea/identificarea lor.
- Există posibilitatea refuzării dreptului de acces în situaţia în care se aplică excepţiile prevăzute de lege. Necesitatea de a restricţiona accesul se poate impune şi în cazul în care există obligaţia de a proteja drepturile şi libertăţile unor terţe persoane, de exemplu dacă în imagini apar şi alte persoane şi nu există posibilitatea de a obţine consimţământul lor sau nu se pot extrage, prin editarea imaginilor, datele personale nerelevante.

17. Auditul securității sistemului de monitorizare video

- Auditul securității sistemului de monitorizare video menţine înscrieri de sistem despre evenimentele produse în activitatea sistemului sau a aplicației, precum şi despre activitatea utilizatorului.
- În conjuncție cu instrumentele şi procedurile respective, auditul securității sistemului de monitorizare video permite de a promova mijloace de ajutor pentru a atinge obiective de securitate: evidența acţiunilor utilizatorului, definirea şi stabilirea responsabilității individuale, reconstrucția evenimentelor, detectarea intruşilor şi problemelor de identificare a evenimentelor.

Auditul securității sistemului de monitorizare video este menit să acorde suport la:

- stabilirea consecutivității acţiunilor utilizatorului sau proceselor;
- stabilirea cînd, cine sau ce a stopat funcționarea normală a sistemului;
- soluționarea problemei de detectare a intrușilor;
- detectarea problemelor de funcționare a sistemului informatic în regim On-Line;

I. **LISTA CU LOCATIILE PENTRU AMPLASAREA CAMERELOR DE SUPRAVEGHERE ÎN CADRUL IMSP „SCMS”**

1. Serviciul Ambulator, Gr.Vieru 22/2.
2. Serviciul Spitalicesc, A. Puskin 51.

II. Locaţiile din împrejurimile clădirilor pentru a proteja spaţiile exterioare;

1. Perimetru Blocului D. Serviciul Ambulator, Gr.Vieru 22/2
2. Perimetru Blocului A,B,C. Serviciul Spitalicesc, A. Puskin 51.

III. Locaţile critice de amplasare a echipamentelor şi sitemelor IT şi de telecomunicaţii:

1. Serviciul Ambulator, Etajul 1,2 „interior”
2. Serviciul Spitalicesc „Parcarea, Garajul, Bl.Alimentar, Farmacia.” Exterior.
3. Serviciul Spitalicesc „Sectia Gereatrie, Terapie intensivă” interior.