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

ORDIN Nr.____76____

mun.Chişinău

„__12__” ____04_____20_16__

„Cu privire la Politica de securitate a 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”, reeșind din cerințele actuale a actelor legislative și normative.

O R D O N:

1. Se nominalizează responsabil de întocmirea, menţinerea, modificarea şi actualizarea politicii de securitate: în mod manual şi pe suport de hîrtie : dna. *Ludmila Ciobotaru ,* în formă digitală d-ul. *Marin Drăgălin* .

1.1. Vor ţine cont de măsurile emise conform ordinului intern Nr_____ „Cu privire la protecţia datelor cu caracter personal”.

2. Şefii de subdiviziuni:

2.1. Vor întreprinde măsurile de securitate stabilite conform regulamentelor de securitate ale fiecărui sistem de evidență care prelucrează date cu caracter personal. În acest sens, la IMSP SCMS se numesc persoanele responsabile privind asigurarea securității datelor medicale cu caracter personal, prelucrarea acestora cu utilizarea tehnologiilor informaționale și în mod manual (pe suport de hîrtie):

Numele Prenumele	**Subdiviziunile**
Ludmila Ciubotaru	Scția informatică și statistică medicală
Tatiana Topală,	Secția Boli Interne-1
Stela Oprea	Secția Boli Interne-2
Alla Zlatovcina	Secția Gereatrie
Liudmila Baraniuc	Secția Boli Interne-4
Victor Celac	Secția Neurologie
Eugen Condrațchii	Secția Chirurgie

Angela Silivanov	Secția Internare
Eduard Roman	Secția Anestezie și reanimare
Anatol Negară	Centrul Național G.G.
Galina Erhan	Secția Consultativ Diagnostic
Corina Pulisca	Secția Centrul Medecină Primară
Grigore Gojan	Centrul Medical Specializat
Margareta Nicu	Secția Fizioterapie și Recuperare
Valentin Diug	Farmacie
Eugenia Rusnac	Laborator Clinic
Otilia Șendrea	Serviciul Radiologie și imagistică
Tatiana Șemetova	Serviciul Diagnostic funțional cardiologie
Tatiana Cravcenco	Serviciul Diagnostic funțional neurologie
Vitali Fuior	Secția Stomatologie
Radu Nastase	Secția Ortopedie
Nionilia Medrigan	Serviciul Ginecologie
Oparin Iustinia	Serviciul Resurse Umane
Pisarenco Maria	Contabil - sef

2.2. În activitatea sa se vor conduce de cerinţele regulamentelor de mai jos:

SECURITATEA MEDIULUI FIZIC ŞI A TEHNOLOGIILOR INFORMAŢIONALE FOLOSITE ÎN PROCESUL PRELUCRĂRII DATELOR CU CARACTER PERSONAL

Măsurile generale de administrare a securităţii informaţionale

În cazul neutilizării temporare a purtătorilor de informaţie pe suport de hîrtie sau electronici (digitali) care conţin date cu caracter personal, aceştia se păstrează în safeuri sau dulapuri metalice care se încuie. Computerele, terminalele de acces şi imprimantele sînt deconectate la terminarea sesiunilor de lucru. Este asigurată securitatea punctelor de primire/expediere a corespondenţei, precum şi securitatea contra accesului neautorizat la aparatele fax şi de copiere. Accesul fizic la mijloacele de reprezentare a informaţiei care conţine date cu caracter personal, în scopul împiedicării vizualizării acesteia de către persoane neautorizate este interzis şi controlat. Mijloacele de prelucrare a datelor cu caracter personal, informaţia care conţine date cu caracter personal sau soft-urile destinate prelucrării datelor cu caracter personal sînt scoase din perimetrul de securitate doar în temeiul unei permisiuni scrise a Directorului.

Securitatea cablurilor de reţea

Cablurile de reţea, prin care se efectuează operaţiuni de prelucrare a datelor cu caracter personal, sînt protejate contra conectărilor nesancţionate sau deteriorărilor. Cablurile sînt separate de cele comunicaţionale pentru a exclude bruiajul. Specialistul în domeniul TI

efectuează controale, nu mai rar decît o dată în lună, în scopul verificării cazurilor de conectare neautorizată la cablurile de reţea.

Controlul instalării şi scoaterii componentelor TI

Se exercită controlul şi evidenţa instalării şi scoaterii mijloacelor de program şi mijloacelor tehnice utilizate în cadrul sistemelor informaţionale de date cu caracter personal. Informaţiile, care conţin date cu caracter personal şi care se conţin pe purtătorii de informaţii, se distrug fizic sau se transcriu şi se nimicesc prin metode sigure.

IDENTIFICAREA ŞI AUTENTIFICAREA UTILIZATORULUI SISTEMULUI INFORMAŢIONAL DE DATE CU CARACTER PERSONAL

Identificarea şi autentificarea utilizatorului

Este efectuată identificarea şi autentificarea utilizatorului sistemelor informaţionale de date cu caracter personal şi a proceselor executate în numele acestui utilizator. Utilizatoriul (persoana care asigură susţinerea tehnică, administrării reţelei şi bazelor de date) are un identificator personal (ID-ul utilizatorului), care nu trebuie să conţină semnalmentele nivelului de accesibilitate al utilizatorului. Pentru confirmarea ID-ului utilizatorului sînt utilizate parole. În cazul în care contractul de muncă/raporturile de serviciu ale utilizatorului au fost încetate, suspendate sau modificate şi noile sarcini nu necesită accesul la date cu caracter personal ori drepturile de acces ale utilizatorului au fost 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 în mod automat în decursul a două săptămîni de la ultimul acces, sau în mod individual la momentul introducerii modificării în raportul de muncă.

Se utilizează autentificarea multifactorială, care include parole complexe, cu includerea simbolurilor, literelor, cifrelor în combinaţie complexă. În mod obligatoriu fiecare parolă conţine una sau mai multe litere scrise cu majusculă. Parola nu va conţine iniţialele sau date care pot caracteriza o anumită persoană (data de naştere, adresă, poreclă, etc.).

Identificarea şi autentificarea echipamentului

Este asigurată posibilitatea identificării şi autentificării echipamentului folosit în operaţiunile de prelucrare a datelor cu caracter personal.

Administrarea identificatorilor utilizatorilor

Administrarea identificatorilor utilizatorilor include:

1) identificarea univocă a fiecărui utilizator;
2) verificarea autenticităţii fiecărui utilizator;
3) obţinerea autorizaţiei de la persoana responsabilă pentru eliberarea ID-ului utilizatorului doar în cazul semnării declaraţiei de confidenţialitate şi trecerii procedurii de instruire;
4) garantarea faptului că ID-ul utilizatorului este eliberat unei persoane determinate concret;
5) dezactivarea contului de utilizator după o perioadă inactivă, stabilită în timp (2 săptămîni);

Asigurarea conexiunii bilaterale în cazul introducerii informaţiei de autentificare a utilizatorilor

Se asigură conexiunea bilaterală a IMSP cu utilizatorul în momentul trecerii de către acesta a procedurilor de autentificare, care nu compromite mecanismul de autentificare.

Utilizarea parolelor în procesul asigurării securităţii informaţionale

Se respectă regulile de asigurare a securităţii informaţionale în cazul alegerii şi folosirii parolelor care includ:

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 cînd sînt prezente indiciile eventualei compromiteri a sistemului sau parolei;
4) alegerea parolelor calitative cu o mărime de minimum 8 simboluri, care nu sînt legate de informaţia cu caracter personal a utilizatorului, nu conţin simboluri identice consecutive şi nu sînt compuse integral din grupuri de cifre sau litere;
5) modificarea parolelor peste intervale de maximum 90 zile;

6) dezactivarea procesului automatizat de înregistrare (cu folosirea parolelor salvate).

Administrarea parolelor utilizatorilor

Se folosesc identificatoare individuale pentru fiecare utilizator şi parole individuale ale acestora pentru asigurarea posibilităţii de stabilire a responsabilităţii. Este asigurată posibilitatea utilizatorilor de a alege şi schimba parolele individuale, inclusiv de activare a procedurii de evidenţă a introducerilor greşite ale acestora. Se asigură blocarea accesului după trei tentative greşite de autentificare. Este asigurată păstrarea istoriilor anterioare în Registrul instituţiei de acordare a identificatorului personal – parola utilizatorului pentru acces la sistemele informaţionale de date cu caracter personal şi prevenirea folosirii repetate a acestora.

ADMINISTRAREA ACCESULUI UTILIZATORILOR

Administrarea accesului

Se implementează mecanisme automate de înregistrare şi evidenţă a persoanelor care au acces sau participă la operaţiunile de prelucrare a datelor cu caracter personal şi care, în caz de necesitate, permit identificarea cazurilor neautorizate de acces sau de prelucrare ilegală a datelor cu caracter personal.

Administrarea conturilor de acces

Este efectuată administrarea conturilor de acces a utilizatorilor care prelucrează date cu caracter personal, inclusiv crearea, activarea, modificarea, revizuirea, dezactivarea şi ştergerea acestora

Acordarea accesului

Este autorizat accesul la sistemele informaţionale de date cu caracter personal în conformitate cu prezenta Politică de securitate persoanelor numite la pct. 1 şi 2.

Revizuirea drepturilor de acces ale utilizatorilor

Drepturile de acces ale utilizatorilor la sistemele informaţionale de date cu caracter personal sînt revizuite cu regularitate pentru asigurarea faptului că nu au fost acordate drepturi de acces neautorizate (maximum peste fiecare şase luni) şi după oricare schimbare de statut al utilizatorului.

Repartizarea obligaţiilor şi învestirea cu minimul de drepturi şi competenţe

Repartizarea obligaţiilor subiecţilor care asigură funcţionarea sistemelor informaţionale de date cu caracter personal este efectuată prin intermediul învestirii cu drepturi/competenţe corespunzătoare de acces, prin ordinul IMSP întocmit în acest sens. Utilizatorii sistemelor informaţionale de date cu caracter personal se învestesc doar cu acele drepturi/competenţe, care sînt necesare pentru realizarea de către ei a obiectivelor stabilite acestora.

Informaţii de avertizare

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

Blocarea sesiunii de lucru

Sesiunea de lucru în sistemul informaţional, destinat prelucrării datelor cu caracter personal, se blochează automat, după maxim 5 minute de perioadă inactivă a utilizatorului fapt care face imposibil accesul de mai departe pînă în momentul cînd utilizatorul nu deblochează sesiunea de lucru prin metoda trecerii repetate a procedurilor de identificare şi autentificare.

Controlul administrării accesului

Se efectuează controlul acţiunilor utilizatorului în vederea evaluării corectitudinii şi conformării operaţiunilor şi acţiunilor efectuate prin intermediul sistemelor informaţionale de date cu caracter personal.

Marcarea documentelor

Informaţia ieşită din sistem, care conţine date cu caracter personal, se marchează, indicîndu-se prescripţii pentru prelucrarea ulterioară şi răspîndirea acesteia, inclusiv indicîndu-se numărul de identificare unic al deţinătorului de date cu caracter personal.

Accesul de la distanţă

Toate metodele de acces de la distanţă la sistemele informaţionale de date cu caracter personal sînt securizate (utilizîndu-se VPN, criptarea, cifrarea etc.), precum şi sînt documentate,

supuse monitorizării şi controlului. Fiecare metodă de acces de la distanţă la sistemele informaţionale de date cu caracter personal se autorizează conform Regulamentelor(anexele 1, 2, 3, 4) şi este permisă doar utilizatorilor, cărora aceasta le este necesar pentru îndeplinirea obiectivelor stabilite.

PROTECŢIA SISTEMELOR INFORMAŢIONALE ŞI COMUNICAŢIILOR ÎN CARE SÎNT PRELUCRATE DATE CU CARACTER PERSONAL

Divizarea programelor aplicative

Se asigură separarea posibilităţilor funcţionale ale utilizatorului de posibilităţile funcţionale de gestionare a sistemelor informaţionale de date cu caracter personal.

Izolarea funcţiilor de securitate

Se asigură izolarea funcţiilor de securitate de funcţiile care nu se atribuie la securitatea sistemelor informaţionale de date cu caracter personal.

Informaţia restantă

Sîntpreîntîmpinate tentativele dezvăluirii neautorizate sau neintenţionate a informaţiei restante care conţine date cu caracter personal, prin intermediul resurselor informaţionale general accesibile.

Protecţia contra refuzului în serviciu

Se asigură protecţia sistemelor informaţionale de date cu caracter personal sau limitate posibilităţile de realizare a atacurilor de diferite tipuri, inclusiv DOS (denial of service) - „refuz în serviciu”.

Priorităţile resurselor

Este asigurată posibilitatea limitării, cu ajutorul mecanismelor de stabilire a priorităţilor, a folosirii resurselor informaţionale în care sînt prelucrate date cu caracter personal.

Asigurarea integrităţii datelor cu caracter personal transmise

Se asigură integritatea datelor cu caracter personal transmise, utilizîndu-se mijloacele de protecţie criptografică.

Asigurarea confidenţialităţii datelor cu caracter personal transmise

Se asigură confidenţialitatea datelor cu caracter personal transmise, utilizîndu-se mijloace de protecţie criptografică a informaţiei.

AUDITUL SECURITĂŢII ÎN SISTEMELE INFORMAŢIONALE DE DATE CU CARACTER PERSONAL

Responsabilul fiecărui sistem informaţional este obligat să întocmească următoarele proceduri obligatorii de audit al sistemului:

1) Se efectuează înregistrarea tentativelor de intrare/ieşire a utilizatorului în sistem, conform următorilor parametri:
a) data şi timpul tentativei intrării/ieşirii;
b) ID-ul utilizatorului;
c) rezultatul tentativei de intrare/ieşire – pozitivă sau negativă.
2) Este efectuată înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative şi proceselor, destinate prelucrării datelor cu caracter personal, înregistrarea modificărilor drepturilor de acces ale utilizatorilor şi statutul obiectelor de acces conform următorilor parametri:
a) data şi timpul tentativei de pornire;
b) denumirea/identificatorul programului aplicativ sau procesului;
c) ID-ul utilizatorului;
d) rezultatul tentativei de pornire – pozitivă sau negativă.

3) Se efectuează înregistrarea tentativelor de obţinere a accesului (de executare a operaţiunilor) pentru aplicaţii şi procese destinate prelucrării datelor cu caracter personal, conform următorilor parametri:
a) data şi timpul tentativei de obţinere a accesului (executare a operaţiunii);
b) denumirea (identificatorul) aplicaţiei sau procesului;
c) ID-ul utilizatorului;
d) specificaţiile resursei protejate (identificator, nume logic, nume fişier, număr etc.);
e) tipul operaţiunii solicitate (citire, înregistrare, ştergere etc.);
f) rezultatul tentativei de obţinere a accesului (executare a operaţiunii) – pozitivă sau negativă.
4) Este efectuată înregistrarea modificărilor drepturilor de acces (competenţelor) utilizatorului şi statutului obiectelor de acces, conform următorilor parametri:
a) data şi timpul modificării competenţelor;
b) ID-ul administratorului care a efectuat modificările;
c) ID-ul utilizatorului şi competenţele acestuia sau specificarea obiectelor de acces şi statutul nou al acestora.

În caz de deranjament al auditului securităţii în sistemele informaţionale de date cu caracter personal sau completării întregului volum de memorie repartizat pentru păstrarea rezultatelor auditului, este informată persoana responsabilă de politica de securitate a datelor cu caracter personal şi întreprinse măsuri în vederea restabilirii capacităţii de lucru a sistemului de audit.

Se efectuează monitorizarea permanentă şi analiza înregistrărilor de audit a securităţii în sistemele informaţionale de date cu caracter personal, în scopul depistării activităţilor neobişnuite sau suspecte de utilizare a acestor sisteme informaţionale, cu întocmirea raportului referitor la cazurile depistării acestor activităţi, stocate în mijloacele electronice de calcul.

Rezultatele auditului securităţii în sistemele informaţionale de date cu caracter personal, care reprezintă operaţiuni de prelucrare a datelor cu caracter personal şi mijloacele de efectuare a auditului, se protejează contra accesului neautorizat prin instituirea măsurilor de securitate adecvate, inclusiv prin asigurarea confidenţialităţii şi integrităţii acestora.

Durata stocării rezultatelor auditului securităţii în sistemele informaţionale de date cu caracter personal se justifică în politica de securitate a datelor cu caracter personal, dar în orice caz acest termen nu este mai mic de 1 an, pentru a fi posibil folosirea acestora în calitate de probe în cazul incidentelor de securitate, unor eventuale investigaţii sau procese judiciare

ASIGURAREA INTEGRITĂŢII INFORMAŢIEI CARE CONŢINE DATE CU CARACTER PERSONAL ŞI A TEHNOLOGIILOR INFORMAŢIONALE

Înlăturarea deficienţelor de soft destinat prelucrăriidatelor cu caracter personal

Se asigură identificarea, protocolarea şi înlăturarea deficienţelor de soft-uri destinate prelucrării datelor cu caracter personal, inclusiv instalarea corectărilor şi pachetelor de reînnoire a acestor soft-uri.

Asigurarea protecţiei contra programelor dăunătoare (viruşilor)

Se asigură protecţia contra infiltrării programelor dăunătoare în soft-urile destinate prelucrării datelor cu caracter personal, măsură care asigură posibilitatea reînnoirii automate şi la timp a mijloacelor de asigurare a protecţiei contra programelor dăunătoare şi signaturilor de virus.

Tehnologiile şi mijloacele de constatare a intruziunilor

Se utilizează tehnologii şi mijloace de constatare a intruziunilor, care permit monitorizarea evenimentelor în sistemele informaţionale de date cu caracter personal şi constatarea atacurilor, inclusiv care asigură identificarea tentativelor folosirii neautorizate a sistemelor informaţionale.

Asigurarea integrităţii soft-urilor şi informaţiei

Se asigură protecţia şi posibilitatea depistării modificării neautorizate a soft-urilor destinate prelucrării datelor cu caracter personal şi informaţiei care conţine date cu caracter personal.

Testarea posibilităţilor funcţionale de asigurare a securităţii sistemelor informaţionale de date cu caracter personal

Se asigură testarea funcţionării corecte a funcţiilor de securitate a sistemelor informaţionale de date cu caracter personal (automat la pornirea sistemului şi lunar pentru verificarea actualizării acestor baze).

COPIILE DE REZERVĂ ŞI RESTABILIREA INFORMAŢIEI CARE CONŢINE DATE CU CARACTER PERSONAL ŞI IT

Copiile de rezervă ale informaţiei care conţine date cu caracter personal

Copiile de siguranţă a informaţiilor enumărate în Regulamentele(anexa 1,2,3,4) care conţin date cu caracter personal şi soft-urilor folosite pentru prelucrările automatizate a datelor cu caracter personal, sunt efectuate zilnic şi finale lunar fiind păstrate în locuri sigure.

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

Procedurile de restabilire a copiilor de siguranţă se actualizează şi se testează cu regularitate, în scopul asigurării eficacităţii acestora.

GESTIONAREA INCIDENTELOR DE SECURITATE A SISTEMELOR INFORMAŢIONALE DE DATE CU CARACTER PERSONAL

Instructajul de reacţionare la incidentele de securitate a sistemelor informaţionale de date cu caracter personal

Persoana care asigură exploatarea sistemelor informaţionale de date cu caracter personal va trece, minimum o dată în an, instruirea referitor la responsabilităţile şi obligaţiile în cazul executării acţiunilor de gestionare şi reacţionare la incidentele de securitate.

În cazul depistării unui incident de securitate se informează neîntîrziat conducerea instituţiei.

Prelucrarea incidentelor include în mod obligator depistarea, analiza, preîntîmpinarea dezvoltării, înlăturarea lor şi restabilirea securităţii iniţiale, precum şi crearea unei pîrghii de evitare a ulterioarelor incidente asemănătoare.

Incidentele de securitate a sistemelor informaţionale de date cu caracter personal se urmăresc şi se documentează în regim permanent.

Anual, către 31 ianuarie, persoana responsabilă de Politica de securitate va prezenta Centrului Naţional pentru Protecţia Datelor cu Caracter Personal raportul generalizat despre incidentele de securitate a sistemelor informaţionale de date cu caracter personal.

3. Executarea prezentului ordin se atribuie vice directorilor: **d-ul. Vasile Parasca, d-ei. Maia Ţiberneac.**

DIRECTOR **Gheorghe ȚURCANU**