Aprobat prin Hotărîrea Consiliului de Administrație

Proces-verbal nr. 13, din 16.02. 2015,

Rector, prof. univ., dr. hab. Gheorghe Popa

REGULAMENTUL PRIVIND PRELUCRAREA INFORMAȚIILOR CE CONȚIN DATE CU CARACTER PERSONAL ÎN SISTEMUL DE EVIDENȚĂ MEDICALĂ

I. DISPOZIŢII GENERALE

1.1. Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență: **Evidența medicală** (în continuare Regulament) este elaborat în vederea implementării în cadrul Instituției Publice Universitatea de Stat „Alecu Russo" din Bălți (în continuare USARB) a prevederilor Legii nr.133 din 8 iulie 2011 privind protecţia datelor cu caracter personal, Legii contabilității nr. 113 din 27 aprilie 2007 și a Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, aprobate prin Hotărîrea Guvernului nr.1123 din 14 decembrie 2010, precum și întru respectarea prevederilor art. 91 - 94 ale Codului muncii al Republicii Moldova.

1.2. Prezentul Regulament reglementează condițiile generale și cerințele față de prelucrarea datelor cu caracter personal ale angajaților USARB în cadrul sistemului de evidență medicală.

II. SCOPUL

2.1. Scopul prelucrării informațiilor ce conțin date cu caracter personal în sistemul de evidență: **Evidența medicală** constă în asigurarea înregistrării informațiilor referitoare la persoanelor care beneficiază de ajutor medical la USARB.

2.2. În cadrul sistemului de evidență: **Evidența medicală** sînt prelucrate următoarele categorii de date cu caracter personal:

- numele, prenumele;
- sexul;
- data şi locul naşterii;
- cetăţenia;
- IDNP;
- imagine;
- situaţia familială;
- semnătura;
- datele din actele de stare civilă;
- numărul de telefon/fax;
- numărul de telefon mobil;
- adresa (domiciliului/reşedinţei);
- adresa e-mail;
- profesia şi/sau locul de muncă;
- numele, prenumele (după caz, patronimicul) persoanelor care se află la întreținerea persoanei respective (membrii familiei, alte rude și persoane, după caz);
- starea de sănătate și viața intimă;
- date genetice;
- caracteristice fizice;
- după caz, alte date necesare îndeplinirii scopului menționat, conform legislației în vigoare.

2.3. Prelucrarea datelor cu caracter personal menționate va fi efectuată pentru realizarea următoarelor scopuri:

a) Întocmirea cartelelor medicale ale salariaților și studenților USARB;

b) Evidența morbidității la locul de muncă și la locul de studii;

c) Evidența îmbolnăvirilor profesionale;

d) Alte scopuri, necesare realizării activităților, care nu contravin legislației.

2.4. Datele cu caracter personal ce fac obiectul reglementării prezentului Regulament vor fi stocate de către responsabilii din cadrul USARB astfel încît să permită identificarea persoanelor vizate strict pe durata necesară realizării scopurilor în care datele sînt prelucrate, iar la expirarea termenului respectiv, înregistrările se vor distruge/șterge, în funcție de suportul pe care au fost efectuate. În cazul obligațiilor expres prevăzute de lege acestea pot rămîne la păstrare primind statut de document de arhivă.

2.5. Orice utilizare a datelor cu caracter personal, introduse în sistemului de evidență: **Evidența medicală** în alte scopuri decît cele menționate mai sus este interzisă.

III. LOCAŢIA ȘI DESCRIEREA SISTEMULUI DE EVIDENȚĂ EVIDENȚA MEDICALĂ

3.1. Datele cu caracter personal conținute în sistemul de evidență: **Evidența medicală** în cadrul USARB se prelucrează și se stochează:

1. pe suport de hîrtie;
2. în format electronic:

a) Software – sistem de operare, care este instalat la computerul medicului-șef;

b) Hardware – calculatoarele, care se află în Biroul medicului-șef din Oficiul medical.

3.2. Mentenanța soft-ului și hard-ului este realizată de către angajații din Departamentul Tehnologii Informaționale al USARB.

III. DURATA DE STOCARE

4.1. Prelucrarea datelor cu caracter personal în sistemul de evidență: **Evidența medicală** se efectuează pe perioada studiilor pentru studenți și pe perioada angajării pentru salariați.

4.2. La expirarea termenelor menționate în punctul 4.1., datele din sistemul de evidență **Evidența medicală** sînt păstrate în formă arhivată, pe perioada stabilită de --- Nomenclatura generală a dosarelor din cadrul USARB, aprobată prin ordinul nr. 01-23 din 26.03.2004, ulterior fiind supuse distrugerii sau ștergerii, în funcție de suportul pe care au fost efectuate.

V. DREPTURILE PERSOANELOR VIZATE

5.1. USARB, în calitate de operator de date cu caracter personal, garantează respectarea drepturilor privind protecția datelor cu caracter personal ce le persoanelor vizate.

5.2. În conformitate cu principiile de protecție a datelor cu caracter personal, persoanele vizate beneficiază de următoarele drepturi: la informare, de acces la date, de intervenție, de opoziție asupra datelor cu caracter personal ce-i vizează, precum și dreptul de a se adresa în justiție.

5.3. Toate persoanele implicate în activitatea de administrare și/sau prelucrare a informațiilor din sistemul de evidență **Evidența medicală** vor respecta procedura de acces la datele cu caracter personal.

5.4. Acordarea dreptului de acces a angajaților la informațiile ce-i vizează se efectuează doar prin solicitarea expresă, în formă scrisă, cu acordul nemijlocit al rectorului USARB. Informațiile furnizate vor fi acordate astfel, încît să nu prejudicieze drepturile terţilor. Persoanele care solicită date cu caracter personal trebuie să indice scopul solicitării, precum și perioada concretă pentru care solicită informațiile.

5.5. Există posibilitatea refuzării dreptului de acces în situaţia în care se aplică excepţiile prevăzute de lege. Necesitatea de a restricţiona accesul se poate impune în cazul în care există obligaţia de a proteja drepturile şi libertăţile unor terţe persoane, de exemplu, dacă în informațiile solicitate apar şi alte persoane şi nu există posibilitatea de a obţine consimţământul acestora sau nu pot fi extrase, prin editare, datele cu caracter personal nerelevante.

VI. MĂSURILE DE PROTECŢIE A DATELOR CU CARACTER PERSONAL PRELUCRATE ÎN SISTEMUL DE EVIDENȚĂ: EVIDENȚA MEDICALĂ

6.1. Măsurile generale de administrare a securităţii informaţionale

6.1.1. În cazul neutilizării temporare a purtătorilor de informaţie pe suport de hîrtie sau electronic care conţin date preluate din sistemul de evidență: Evidența medicală, aceştia se păstrează în safeuri care se încuie.

6.1.2. La terminarea sesiunilor de lucru, computerele şi imprimantele se deconectează de la rețeaua electrică.

6.1.3. Operatorul asigură securitatea punctelor de primire și expediere a corespondenţei, precum şi securitatea contra accesului neautorizat la aparatele de copiere.

6.1.4. Accesul fizic la mijloacele de reprezentare a informaţiei preluate din sistemul de evidență: Evidența medicală este blocat împotriva vizualizării de către persoane neautorizate.

6.1.5. Mijloacele de prelucrare a informațiilor preluate din sistemul de evidență: Evidența medicală sau soft-urile destinate prelucrării acestora sînt scoase din perimetrul de securitate doar în baza permisiunii scrise a operatorului.

6.1.6. Scoaterea şi introducerea mijloacelor de prelucrare a informațiilor din sistemul de evidență: Evidența medicală din/în perimetrul de securitate se înregistrează în registru.

6.2. Măsurile de protecţie a datelor cu caracter personal, prelucrate în sistemul de evidență: Evidența medicală, se înfăptuiesc ţinînd cont de necesitatea asigurării confidenţialităţii și integrității acestora, prin protecţie în formă manuală, electronică şi externă.

6.3. Cerințe speciale față de marcare**:** toate informațiile ieşite din sistemul de evidență: Evidența medicală, care conţin date cu caracter personal, sînt supuse marcării, cu indicarea prescripţiilor pentru prelucrarea ulterioară şi răspîndirea acestora, inclusiv cu indicarea numărului de identificare unic al operatorului de date cu caracter personal.

6.4. Accesul în biroul unde este amplasat sistemul de evidență: Evidența medicală este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară şi doar în timpul orelor de program. Accesul în birou este posibil doar cu autorizarea de acces și cheia de la lacătul mecanic.

6.5. Biroul nu este lăsat niciodată fără supraveghere la ieșirea în exterior, ușa biroului se încuie cu lacătul.

6.6. Înainte de acordarea accesului fizic la sistemul de evidență: Evidența medicală, se verifică competenţele de acces.

6.7. Registrele de monitorizare se păstrează minimum un an, la expirarea termenului indicat, acestea se lichidează, iar datele şi documentele ce se conţin în registrul supus lichidării se transmit în arhivă.

6.8. Perimetrul de securitate se consideră perimetrul biroului în care este amplasat sistemul de evidență: Evidența medicală, fiind integru din punct de vedere fizic.

6.9. Zilnic, se inspectează perimetrul de securitate al clădirii și al biroului, unde este amplasat sistemul de evidență: Evidența medicală, din punct de vedere fizic.

6.10. Computerele sînt amplasate în locuri cu acces limitat pentru persoane străine.

6.11. Uşile şi ferestrele sînt încuiate în cazul în care în încăpere lipsesc angajații autorizați de administrarea sistemului.

6.12. Amplasarea sistemului de evidență: **Evidența medicală** răspunde necesităţii asigurării securităţii acestora contra accesului nesancţionat, furturilor, incendiilor, inundaţiilor şi altor posibile riscuri.

6.13. Securitatea electroenergetică: este asigurată securitatea echipamentului electric utilizat pentru menţinerea funcţionalităţii sistemului de evidență: **Evidența medicală**, a cablurilor electrice, inclusiv protecţia acestora contra deteriorărilor şi conectărilor nesancţionate. În cazul apariţiei situaţiilor excepţionale, de avarie sau de forţă majoră, este asigurată posibilitatea deconectării electricităţii la sistemele de evidență contabilă, inclusiv posibilitatea deconectării oricărui component TI.

6.14. Computerele, unde este amplasat fizic sistemul de evidență: Evidența medicală, dispun de UPS-uri, care sînt folosite pentru încheierea corectă a sesiunii de lucru a sistemelor (componentelor) în cazul deconectării de la sursa de alimentare cu energie electrică.

6.15. Securitatea cablurilor de reţea: cablurile de reţea, prin care se efectuează operaţiunile de transmitere a datelor preluate din sistemul de evidență: Evidența medicală, sînt protejate contra conectărilor nesancţionate sau deteriorărilor. Pentru a exclude bruiajul, cablurile de tensiune sînt separate de cele comunicaţionale.

6.16. Securitatea antiincendiară a sistemului de evidență contabilă: biroul unde este amplasat sistemul de evidență: Evidența medicală este dotat cu echipament antiincendiar și corespunde cerințelor și normelor antiincendiare în vigoare.

6.17. Controlul instalării şi scoaterii componentelor TI: se efectuează controlul şi evidenţa instalării şi scoaterii mijloacelor de program, mijloacelor tehnice şi celor tehnice de program, utilizate în cadrul sistemului de evidență contabilă. La expirarea termenului de păstrare, informaţiile, care conţin date cu caracter personal şi care se conţin pe purtătorii de informaţii, se distrug.

VII. IDENTIFICAREA ŞI AUTENTIFICAREA UTILIZATORULUI SISTEMULUI DE EVIDENȚĂ: EVIDENȚA MEDICALĂ

7.1. Este efectuată identificarea şi autentificarea utilizatorilor informațiilor preluate din sistemele de evidență şi a proceselor executate în numele acestor utilizatori.

7.2. Toţi utilizatorii (inclusiv personalul care asigură mentenanța tehnică, administratorii de reţea, programatorii şi administratorii bazelor de date) au un identificator personal (ID-ul

utilizatorului), care nu trebuie să conţină semnalmentele nivelului de accesibilitate al utilizatorului.

7.3. Pentru confirmarea ID-ului utilizatorului sînt utilizate parole. Utilizarea parolelor în procesul asigurării securităţii informaţionale: pe lîngă cerințele de păstrare a confidențialității parolelor, este interzisă înscrierea acestora pe suport de hîrtie, cu excepția cazului de asigurare a securității păstrării acesteia (plasarea înscrisurilor în safeu). La momentul introducerii, parolele nu se reflectă în clar pe monitor.

7.4. Se efectuează modificarea parolelor de fiecare dată cînd sînt depistați indicii unei eventuale compromiteri a sistemului sau parolei.

7.5. Întru asigurarea posibilităţii de stabilire a responsabilităţii fiecărui utilizator, sînt folosite identificatori şi parole individuale ale acestora. Este asigurată posibilitatea utilizatorilor de a alege şi schimba parolele individuale, inclusiv de activare a procedurii de evidenţă a introducerilor greşite ale acestora. După trei tentative greşite de autentificare, accesul este blocat, în mod automatizat.

7.6. Se asigură, pentru o perioadă de 1 */un/* an, păstrarea istoriilor anterioare ale parolelor în formă de hash a utilizatorilor şi prevenirea folosirii repetate a acestora.

7.7. În cazul în care raporturile de muncă ale utilizatorului au încetat, au fost suspendate sau modificate, și, ca urmare, noile sarcini nu necesită accesul la datele cu caracter personal, precum și în cazul de modificare a drepturilor de acces ale utilizatorului, abuz al utilizatorului de autorizații de acces primite în scopul comiterii unei fapte prejudiciabile, absență a utilizatorului la postul de muncă pe parcursul unei perioade îndelungate (mai mult de 3 luni), codurile de identificare şi autentificare se revocă sau se suspendă.

7.8. Se efectuează, prin mijloace automatizate de suport, administrarea conturilor de acces a utilizatorilor care prelucrează datele cu caracter personal în sistemul de evidență: Evidența medicală, inclusiv crearea, activarea, modificarea, revizuirea, dezactivarea şi ştergerea acestora. Acţiunea conturilor de acces a utilizatorilor temporari, care prelucrează date cu caracter personal înregistrate în sistemul de evidență: Evidența medicală, încetează automat la expirarea perioadei stabilite în timp (pentru fiecare tip de cont de acces în parte). Se dezactivează automat, după o perioadă de maxim 1 */una/* lună, conturile de acces ale utilizatorilor neactivi, care prelucrează informațiile din sistemul de evidență: Evidența medicală. Se folosesc mijloace automatizate de înregistrare şi informare despre crearea, modificarea, dezactivarea şi încetarea acţiunii conturilor de acces.

7.9. În scopul depistării și evitării cazurilor de acordare a drepturilor de acces neautorizat, se revizuiește cu regularitate, maximum la fiecare şase luni şi după oricare schimbare a statutului utilizatorului, drepturile de acces ale utilizatorilor la sistemul de evidență: Evidența medicală.

7.10. Folosirea tehnologiilor fără fir, echipamentelor portative și mobile se autorizează de persoanele responsabile.

7.11. Se impun limite în privinţa persoanelor care au dreptul:
a) să vizualizeze informațiile stocate în sistemul de evidență: Evidența medicală;
b) să copieze, să descarce, să şteargă sau să modifice orice informație stocată.

7.12. Toţi angajații cu drepturi de acces beneficiază de o instruire inițială în domeniul protecţiei datelor cu caracter personal.

7.13. Orice activitate de dezvăluire a datelor cu caracter personal către terţi este documentată şi supusă unei analize riguroase în prealabil privind scopul și temeiul legal a intențiilor de dezvăluire a unui anumit volum de date cu caracter personal.

7.14. Orice încălcare a securităţii în ceea ce priveşte sistemul de evidență: Evidența medicală este supusă documentării, iar persoana responsabilă de realizarea politicii de securitate este informată în legătură cu acest lucru cît de urgent posibil.

7.15. Înainte de acordarea accesului în sistem, utilizatorii sînt informaţi despre faptul că folosirea sistemului de evidență contabilă este controlată şi că folosirea neautorizată a acestora este sancționată în conformitate cu legislaţia civilă, contravențională și penală.

VIII. AUDITUL SECURITĂŢII ÎN SISTEMELE DE EVIDENȚĂ: EVIDENȚA MEDICALĂ

8.1. Se organizează generarea înregistrărilor de audit a securităţii în sistemul de evidență: Evidența medicală pentru evenimentele, indicate în lista corespunzătoare, supuse auditului.

8.2. 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.

8.3. Se efectuează înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative şi proceselor, destinate prelucrării informațiilor din sistemele de evidență contabilă, 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 al procesului;
c) ID-ul utilizatorului;
d) rezultatul tentativei de pornire – pozitivă sau negativă.

8.4. Se efectuează înregistrarea tentativelor de obţinere a accesului (de executare a operaţiunilor) pentru aplicaţii şi procese destinate prelucrării informațiilor din sistemul de evidență: Evidența medicală, conform următorilor parametri:
a) data şi timpul tentativei de obţinere a accesului (executare a operaţiunii);
b) denumirea (identificatorul) aplicaţiei sau a 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.

8.5. Se efectuează 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.

8.6. Se efectuează înregistrarea ieşirii din sistemul de evidență: Evidența medicală, înregistrarea modificărilor drepturilor de acces ale subiecţilor şi statutul obiectelor de acces, conform următorilor parametri:
a) data şi timpul eliberării;
b) denumirea informaţiei şi căile de acces la aceasta;
c) specificarea echipamentului (dispozitivului) care a eliberat informaţia (numele logic);
d) ID-ul utilizatorului care a solicitat informaţia;
e) volumul documentului eliberat (numărul paginilor, filelor, copiilor) şi rezultatul eliberării – pozitiv sau negativ.

8.7. Cazurile de deranjament al auditului securităţii în sistemul de evidență: Evidența medicală sau completării întregului volum de memorie repartizat pentru păstrarea rezultatelor auditului, sînt aduse la cunoștința persoanei responsabile de politica de securitate a datelor cu caracter personal, care întreprinde măsuri în vederea restabilirii capacităţii de lucru a sistemului de audit.

8.8. Rezultatele auditului securităţii în sistemul de evidență: Evidența medicală (operaţiunile de prelucrare a informațiilor şi mijloacele de efectuare a auditului), se protejează contra accesului neautorizat prin aplicarea măsurilor de securitate adecvate și asigurarea confidenţialităţii şi integrităţii acestora.

8.9. Durata minimă a stocării rezultatelor auditului securităţii în sistemul de evidență: Evidența medicală constituie 2 */doi/* ani, în scopul asigurării posibilității de folosire a acestora în calitate de probe în cazul incidentelor de securitate, unor eventuale investigaţii sau procese judiciare. În cazul în care investigările sau procesele judiciare se prelungesc, rezultatele auditului se păstrează pe toată durata acestora.

IX. ASIGURAREA INTEGRITĂŢII INFORMAŢIILOR DIN SISTEMUL DE EVIDENȚĂ: EVIDENȚA MEDICALĂ

9.1. Se asigură identificarea, protocolarea şi înlăturarea deficienţelor de soft-uri destinate prelucrării informațiilor din sistemul de evidență: Evidența medicală, inclusiv instalarea corectărilor şi pachetelor de reînnoire a acestora, protecţia contra infiltrării programelor dăunătoare în soft-uri, măsuri care asigură posibilitatea reînnoirii automate şi la timp a mijloacelor de asigurare a protecţiei contra programelor dăunătoare şi signaturilor de virus.

9.2. Se utilizează tehnologii şi mijloace de constatare a intrărilor ilegale, ce permit monitorizarea evenimentelor şi constatarea atacurilor, inclusiv asigură identificarea tentativelor folosirii neautorizate a informațiilor din sistemul de evidență: Evidența medicală.

9.3. Se asigură testarea funcţionării corecte a componentelor de securitate a sistemului de evidență Evidența medicală (automat – la pornirea sistemului, şi după caz – la solicitarea persoanei responsabile de politica de securitate a prelucrării datelor cu caracter personal).

9.4. Copiile de siguranță: reieşind din volumul prelucrărilor efectuate, individual, se stabileşte de către operator intervalul de timp în care se execută copiile de siguranţă a informaţiilor din sistemul de evidență: Evidența medicală şi soft-urilor folosite pentru prelucrările automatizate a acestora. Copiile de siguranţă se testează în scopul verificării siguranţei purtătorilor de informaţii şi integrităţii informaţiei indicate. Procedurile de restabilire a copiilor de siguranţă se actualizează şi se testează cu regularitate, în scopul asigurării eficacităţii acestora.

X. GESTIONAREA INCIDENTELOR DE SECURITATE A SISTEMULUI DE EVIDENȚĂ EVIDENȚA MEDICALĂ

10.1. Persoanele care asigură exploatarea sistemului de evidență Evidența medicală trec, minimum o dată în an, instruirea cu privire la responsabilităţile şi obligaţiile în cazul executării acţiunilor de gestionare şi reacţionare la incidentele de securitate.

10.2. Prelucrarea incidentelor de securitate include depistarea, analiza, preîntîmpinarea dezvoltării, înlăturarea lor şi restabilirea securităţii. Se monitorizează şi documentează, în mod permanent, incidentele de securitate în sistemul de evidență: Evidența medicală.

10.3. Persoanele care se fac vinovate de încălcarea normelor privind obţinerea, păstrarea, prelucrarea şi protecţia informațiilor din sistemul de evidență: Evidența medicală poartă răspundere civilă, contravențională și penală.

XI. DISPOZIŢII FINALE

11.1. Prezentul Regulament este revizuit şi ulterior aprobat de către Consiliul de Administrație al USARB periodic, însă cel puțin o dată în an, precum și la necesitate.

11.2. Prezentul Regulament se completează cu prevederile legislației în vigoare.

11.3. Regulamentul este adus la cunoştinţa angajaților contra semnăturii.

11.4. Modificarea şi completarea prezentului Regulament se face în modul stabilit pentru aprobarea lui.