



Politica de Securitate a Institutului de Urgență pentru Boli Cardiovasculare și Transplant din Târgu Mureș

Elaborata în baza deciziei nr.101 din 2008, a Autorității Naționale de Cercetare Științifică, privind procedura emiterii autorizației pentru prelucrarea datelor cu caracter personal privind starea de sănătate, în condițiile art.9, alin.(3) și(4) din Legea nr. 677 din 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date.

1. Introducere

În acord cu prevederile din prezentul act, **informațiile medicale** ale pacienților internați sau tratați în ambulatorul integrat, reprezintă resurse scrise, informatice, de comunicare și tehnice, create și deținute de Institutul de Urgență pentru Boli Cardiovasculare și Transplant din Târgu Mureș, sunt bunuri strategice ale instituției, regasite în arhiva scrisă, electronică și tehnică, care trebuie administrate ca resurse ale statului român și cu respectarea legilor în vigoare.

Compromiterea securității acestor informații poate afecta capacitatea Institutului de Urgență pentru Boli Cardiovasculare și Transplant din Târgu Mureș de a oferi servicii medicale, informatice și de comunicații, poate conduce la fraude sau distrugerea datelor, la violarea drepturilor individului la viața privată și a clauzelor contractuale, divulgarea secretelor de serviciu și profesionale, la afectarea credibilității instituției în fața pacienților și partenerilor săi.

Această politică este stabilită astfel încât:

- Să fie în conformitate cu statutul, regulamentele, legile și alte documente oficiale în vigoare privind administrarea resurselor informatice publice,
- Să stabilească practici prudente și acceptabile privind utilizarea resurselor scrise, informatice, de comunicații și tehnice, ale Institutului de Urgență pentru Boli Cardiovasculare și Transplant din Târgu Mureș,
- Să instruiască utilizatorii care au drept de folosire a resurselor informatice și de comunicații privind responsabilitățile asociate unei astfel de utilizări.

2. Audiența Politicii de Securitate

Politica de securitate a informațiilor medicale, resurselor informatice și a celor de comunicare ale Institutului de Urgență pentru Boli Cardiovasculare și Transplant din Târgu Mureș se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice informație medicală, resursă informatică și de comunicații ce aparține instituției.

Următoarele entități și utilizatori sunt vizați în mod distinct de prevederile acestui document:

- Angajații cu contract de muncă pe perioadă determinată sau nedeterminată care au acces fizic la datele personale și medicale ale pacienților precum și la sistemul informațional și de comunicații al Institutului;
- Colaboratorii Institutului de Urgență pentru Boli Cardiovasculare și Transplant din Târgu Mureș care, în baza prevederilor contractelor încheiate, au acces la datele personale

și medicale ale pacienților precum și la sistemul informațional și de comunicații al Institutului;

- Medicii rezidenți aflați în stagiul de pregătire conform curriculei de pregătire și studenții care efectuează stagii / cursuri la Institutul de Urgență pentru Boli Cardiovasculare și Transplant Târgu Mureș, conform contractelor de colaborare încheiate cu unitatea de învățământ;

- Persoane juridice, entități sau organizații care au acces la datele personale și medicale ale pacienților precum și la sistemul informațional și de comunicații al Institutului (Ministerul Sănătății – Centrul Național pentru Organizarea și Asigurarea Sistemului Informațional și Informatic în Domeniul Sănătății, Agenția Națională de Transplant, Casa Națională de Asigurări de Sănătate, Casa Județeană de Asigurări de Sănătate, Școala Națională de Sănătate Publică și Management Sanitar, societăți de asigurări).

- Administratori autorizați prin lege ai Registrelor naționale de Boli, prevăzute de legislația în vigoare (ex. Registrul Național de Transplant, Registrul European al Cardiopatiilor Congenitale - EACTS)

- Asociații profesionale naționale și internaționale la care acestea sunt afiliate, în specialitățile medicale: cardiologie, chirurgie cardiovasculară, ATI, neonatologie, (ex. Societatea Română de Cardiologie, Societatea Română de Chirurgie cardiovasculară, Societatea Română de Anestezie și Terapie Intensivă, Societatea Europeană de Cardiologie, Societatea Europeană de Chirurgie Cardio-Toracică EACTS, etc)

- Mass-media, numai cu acordul pacientului, cu respectarea Legii nr.46/ 2003 a drepturilor pacientului și a Regulamentului de Ordine Interioară al IBCVT Tg. Mureș.

3. Scopul Politicii de Securitate

Politica de securitate a resurselor informatice și de comunicații are ca scop asigurarea integrității, confidențialității și disponibilității informației. În contextul documentului de față, confidențialitatea se referă la protecția datelor împotriva accesului neautorizat și utilizarea și prelucrarea lor neautorizată.

Documentele medicale create, ale pacienților internați și/sau monitorizați în ambulatoriu integrat al IBCvT Tg. Mureș, completate, trimise, primite sau arhivate precum și fișierele electronice create, trimise, primite sau stocate pe sistemele de calcul aflate în proprietatea, administrarea sau în custodia și sub controlul Institutului de Urgență pentru Boli Cardiovasculare și Transplant din Târgu Mureș, sunt proprietatea Institutului în condițiile legilor în vigoare. Utilizatorul răspunde personal de confidențialitatea datelor încredințate prin procedurile de acces la resursele informatice și de comunicații.

Integritatea se referă la măsurile și procedurile utilizate pentru protecția datelor împotriva modificărilor sau distrugerii neautorizate.

Disponibilitatea se asigură prin funcționarea continuă a tuturor componentelor sistemului care administrează resursele informatice și de comunicații. Diverse documente medicale precum și fișiere electronice aflate în proprietatea Institutului vor avea nevoie de nivele diferite de securitate în funcție de impactul sau daunele produse ca urmare fie a nefuncționării corespunzătoare sistemului de administrare al resurselor informatice și de comunicații, fie ca urmare a ajungerii acestora în proprietatea utilizatorilor neautorizați.

Politica de securitate are ca scop, de asemenea, stabilirea cadrului necesar pentru elaborarea regulamentelor și procedurilor de securitate. Acestea sunt obligatorii pentru toți utilizatorii resurselor informatice și de comunicații enumerați la Capitolul 2.

4. Definiții

Strategia de Securitate: este documentul care definește liniile generale și obiectivele Institutului de Urgență pentru Boli Cardiovasculare și Transplant din Târgu Mureș din punct de vedere al protecției tuturor resurselor critice. Este o strategie concepută pe termen lung și urmărește îndeaproape interesul managementului Institutului pentru asigurarea protecției propriilor date și informații, întreținerea unui nivel de protecție adecvat, adaptarea acestuia la provocările mediului înconjurător și îmbunătățirea permanentă a sistemului de securitate. Strategia de securitate este susținută de management, ca expresie incotestabilă a voinței conducerii Institutului de a proteja resursele informaționale.

Politica de Securitate este instrumentul care preia principiile exprimate în Strategia de Securitate și le distribuie în mod explicit către întreaga instituție. Politica de Securitate constă din prezentul set de reguli și practici care reglează modul în care Institutul folosește, administrează, protejează și distribuie informațiile sensibile. Rolul politicii de Securitate este de a informa pe toți care activează în cadrul Institutului de Urgență pentru Boli Cardiovasculare și Transplant din Târgu Mureș asupra modului în care trebuie să se comporte privind protecția informației, care este poziția conducerii referitor la acest subiect și care sunt acțiunile specifice în funcție de situațiile apărute. Politica de Securitate are în vedere toate activitățile din cadrul Institutului și reglementează modul în care sunt tratate datele și informațiile secrete și strict secrete.

Planul de Securitate descrie în mod concret procesele și activitățile ce trebuie desfășurate pentru a îndeplini obiectivele Strategiei de Securitate și a realiza sistemul de protecție necesar.

Documente medicale: toate documentele care conțin date personale și medicale aflate în administrarea Institutului, fie ca au fost emise, completate și prelucrate de către utilizatorii enumerați la Capitolul 2 sau au o altă proveniență dar se află pentru o perioadă de timp în circuitul de documente al Institutului.

Resurse informatice și de comunicații: toate dispozitivele de tipărire/imprimare, dispozitive de afișare, unități de stocare și toate activitățile asociate sistemelor de calcul care implică utilizarea oricărui dispozitiv capabil să transmită, stocheze, administreze date electronice, incluzând, dar nu limitat la: mainframe-uri, servere, calculatoare personale, calculatoare portabile, asistenți digitali personali, sisteme de procesare distribuită, echipament de laborator și medical, resurse de telecomunicații, medii de rețea, telefoane, faxuri, imprimante și alte accesorii. La acestea se adaugă procedurile, echipamentul, facilitățile, programele și datele care sunt proiectate, construite, puse în funcțiune și menținute pentru a crea, colecta, înregistra, procesa, stoca, primi, afișa și transmite informația.

Centrul de comunicații și informatizare: centrul responsabil la nivelul instituției cu administrarea resurselor informatice și de comunicații are ca scop stabilirea în mod clar a responsabilității privind crearea, modificarea și aprobarea regulamentelor privind activitățile de administrare și utilizare a resurselor informatice și de comunicații, reprezentat prin administratorul de rețea.

Utilizator: O persoană, o aplicație automatizată sau proces utilizator autorizat de către Institutul de Urgență pentru Boli Cardiovasculare și Transplant din Târgu Mureș, în conformitate cu procedurile și regulamentele în vigoare, să folosească resursele informatice și de comunicații.

Abuz de privilegii: Orice acțiune întreprinsă în mod voit de un utilizator, care vine în contradicție cu regulamentele Institutului de Urgență pentru Boli Cardiovasculare și Transplant din Târgu Mureș și/sau legile în vigoare, inclusiv cazul în care, din punct de vedere tehnic, nu se poate preveni îmfăptuirea de către utilizator a acțiunii respective.

Furnizor: Persoană fizică sau juridică ce oferă bunuri sau servicii Institutului de Urgență pentru Boli Cardiovasculare și Transplant din Târgu Mureș în baza unui contract comercial sau de colaborare.

Informația medicală: Reprezintă resurse scrise, informatice, de comunicare și tehnice, create și deținute de Institutul de Urgență pentru Boli Cardiovasculare și Transplant din Târgu

Mureș sunt bunuri strategice ale instituției, regăsite în arhiva scrisă, electronică și tehnică, care trebuie administrate ca resurse ale statului român și cu respectarea legilor în vigoare.

5. Clasificarea informațiilor

Clasificarea informațiilor este necesară pentru a permite atât alocarea resurselor necesare administrării și protejării acestora cât și pentru a determina potențialele pierderi ca urmare a modificărilor, pierderii/distrugerii sau divulgării acestora.

Pentru a asigura securitatea și integritatea informațiilor, acestea se împart în trei categorii principale:

- Informații publice
- Informații secrete
- Informații strict secrete (confidențiale)

Centrul de comunicații și informatizare precum și conducerea Secțiilor Clinice/laboratoare/compartimente/servicii ce aparțin Institutului răspund de evaluarea periodică a schemei de clasificare a informațiilor. Toate informațiile din Institutul de Urgență pentru Boli Cardiovasculare și Transplant din Târgu Mureș trebuie să se regăsească în una din următoarele categorii:

a) Informații publice: Acestea sunt informațiile accesibile oricărui utilizator din interiorul sau exteriorul Institutului de Urgență pentru Boli Cardiovasculare și Transplant din Târgu Mureș, conform Legii nr. 544/2001. Divulgarea, utilizarea neautorizată sau distrugerea acestora nu produce efecte asupra instituției sau aceste efecte sunt ne semnificative. Utilizatorii care furnizează aceste informații sunt responsabili de asigurarea integrității și disponibilității acestora în raport cu cerințele Institutului de Urgență pentru Boli Cardiovasculare și Transplant din Târgu Mureș.

Exemple: Informațiile privind orarul de funcționare, informațiile aflate pe pagina de internet a Institutului, știrile de presă referitoare la Institut.

b) Informații secrete: În această categorie se includ informațiile care datorită valorii economice nu trebuie făcute publice. Se includ aici și informațiile pe care Institutul de Urgență pentru Boli Cardiovasculare și Transplant din Târgu Mureș trebuie să le protejeze conform legislației în vigoare. Datorită valorii economice asociate, aceste date trebuie distruse dacă au fost făcute publice. Aceste date vor fi copiate și distribuite în cadrul Institutului doar utilizatorilor autorizați. Distribuirea acestor informații de către utilizatorii autorizați trebuie să se facă pe baza unei clauze de confidențialitate.

Exemple: informații medicale din fișele pacienților, clauze contractuale ale angajaților, conturi și parole de utilizator folosite pe echipamentele de calcul ale instituției.

c) Informații strict secrete sau confidențiale: În această categorie se includ toate informațiile care datorită valorii economice nu trebuie făcute publice. Divulgarea, utilizarea sau distrugerea acestor date poate intra sub incidența Codului Civil, Penal sau legislației fiscale, Codului Muncii.

Accesul la aceste informații va fi restricționat. Datele strict secrete nu pot fi copiate, distribuite sau șterse fără acordul scris al conducerii Institutului.

Exemple: datele cu caractere personale ale pacienților, procedurile medicale efectuate, cheile criptografice, conturile de administrator de pe serverele instituției.

6. Atribuții și responsabilități

Atribuțiile manageriale privind politica de securitate includ următoarele:

- managementul Institutului se va asigura ca persoanele enumerate la Capitolul 2 au luat la cunoștință de prezenta Politică de Securitate și că prevederile acesteia, precum și a regulamentelor și procedurilor asociate acestei politici sunt respectate întocmai;
- managementul Secțiilor clinice/laboratoare/compartimente/servicii aparținând Institutului va monitoriza circulația și evidența documentelor medicale conform regulamentelor și a procedurilor asociate;
- administratorii de rețea/sistem/baze de date trebuie să asigure existența jurnalelor de tip log și a traseelor auditării pentru orice tip de acces în sistem conform regulamentelor sau procedurilor asociate;
- administratorii de rețea/sistem/baze de date trebuie să asigure activarea tuturor mecanismelor de securitate;

Atribuțiile Centrului de comunicații și informatizare includ următoarele:

- elaborează și propune modificări ale politicii de securitate a sistemului de resurse informatice și de comunicare;
- elaborează și propune pentru aprobare regulamentele și procedurile de securitate a resurselor informatice și de comunicații în conformitate cu politica de securitate a acestora;
- elaborează proceduri pentru autentificarea și identificarea utilizatorilor resurselor informatice și de comunicații;
- tratează incidente de securitate în scopul minimizării efectului distructiv al acestora asupra resurselor informatice și de comunicații;
- facilitează evaluărilor legale, răspunde cerințelor de tipul "cele mai bune practici" pe măsură ce acestea devin recunoscute.

Atribuții ale utilizatorilor:

- să cunoască și să respecte prevederile Politicii de Securitate a resurselor informatice și de comunicații;
- să cunoască și să respecte prevederile tuturor regulamentelor și procedurile privind securitatea resurselor informatice și de comunicații;
- să răspundă direct de securitatea și conținutul informațiilor și resursele informatice și de comunicații încredințate direct sau indirect.

Alte atribuții:

- toți partenerii Institutul de Urgență pentru Boli Cardiovasculare și Transplant din Târgu Mureș (furnizori, studenți, colaboratori etc.) trebuie să accepte și să respecte prezentul document și regulamentele specifice privind resursele informatice și de comunicații.

7. Confidențialitate

1. Documentele medicale create, completate, primite sau arhivate folosind resursele informatice și de comunicații ale Institutului de Urgență pentru Boli Cardiovasculare și Transplant din Târgu Mureș și aflate în proprietatea și administrarea sau în custodia acestuia pot fi accesate doar de către angajații autorizați ai Institutului;

2. Fișierele electronice create, trimise, primite sau stocate folosind resursele informatice și de comunicații administrate sau în custodia și sub controlul Institutul de Urgență pentru Boli Cardiovasculare și Transplant din Târgu Mureș pot fi accesate doar de către angajații autorizați din cadrul Institutului;

3. În scopul administrării resurselor informatice și de comunicații și pentru asigurarea securității acestora, personalul autorizat poate revizui sau utiliza orice informație arhivată,

stocată sau transportată prin sistemele Resurselor informatice și de comunicații în conformitate cu legile în vigoare. În aceleași scopuri, este posibilă monitorizarea activității utilizatorilor (de exemplu, dar fără a se limita la, verificarea prezenței și activității utilizatorilor în sistemul informatic sau sit-uri web vizitate);

4. Utilizatorii trebuie să raporteze orice slăbiciune în sistemul de securitate al Institutul de Urgență pentru Boli Cardiovasculare și Transplant din Târgu Mureș, orice incident de posibilă întrebuițare greșită sau încălcare a acestui regulament (prin contactarea Centrului de comunicații și informatizare);

5. Un număr restrâns de utilizatori au autorizația de a transmite informații în clar sau criptate în exteriorul Institutului, motiv pentru care aceștia vor fi nominalizați și instruiți în mod specific pentru a asigura păstrarea confidențialității informațiilor transmise din interiorul instituției către exteriorul acesteia (Exemple: raportări lunare, trimestriale și anuale către Ministerul Sănătății, Casa Județeană de Asigurări, Școala Națională de Sănătate Publică și Management Sanitar, Direcția de Sănătate Publică);

6. Utilizatorilor li se interzice accesarea informațiilor pentru care nu au autorizare sau pentru care nu au consimțământ explicit;

7. Utilizatorii nu pot divulga informațiile la care au sau au avut acces ca urmare a unei vulnerabilități a sistemului, această regulă fiind valabilă și după ce utilizatorul a încheiat relațiile cu Institutul de Urgență pentru Boli Cardiovasculare și Transplant din Târgu Mureș.

8. Utilizatorii sunt obligați să se asigure că toate informațiile confidențiale ale Institutul de Urgență pentru Boli Cardiovasculare și Transplant din Târgu Mureș se transmit în așa fel încât să se asigure confidențialitatea și integritatea acestora.

8. Reguli de utilizare acceptabilă a resurselor informatice și de comunicații

- utilizarea resurselor informatice și de comunicații se face numai în interes de serviciu;
- utilizatorii trebuie să anunțe Centrul de comunicații și informatizare în cazul în care se observă orice problemă/breșă în sistemul de securitate din cadrul Centrului de comunicații și informatizare cât și orice posibilă întrebuițare greșită sau încălcare a regulamentelor în vigoare;
- utilizatorii, prin acțiunile lor, nu trebuie să încerce să compromită protecția sistemelor informatice și de comunicații și nu trebuie să desfășoare, deliberat sau accidental, acțiuni care pot afecta confidențialitatea, integritatea și disponibilitatea informațiilor de orice tip în cadrul resurselor informatice și de comunicații ale Centrului de comunicații și informatizare;
- utilizatorii nu trebuie să încerce să obțină acces la date sau programe din resursele informatice și de comunicații pentru care nu au autorizație sau consimțământ explicit;
- utilizatorilor li se interzice divulgarea sau înstrăinarea numele de conturi, parole, dispozitive pentru autentificare sau orice dispozitive și/sau informații similare utilizate în scopuri de autorizare și identificare;
- utilizatorilor li se interzice să facă copii neautorizate ale documentelor sau să distribuie materiale protejate prin legile privind proprietatea intelectuală și a dreptului de autor;
- utilizatorii nu vor instala / utiliza pe echipamentele de calcul proprietate a Institutului programe neautorizate fără aprobarea Centrului de comunicații și informatizare;
- utilizatorii nu vor degrada performanțele sistemelor ce alcatuiesc resursele informatice și de comunicații;
- utilizatorii autorizați nu vor împiedica accesul unui alt utilizator autorizat la resursele informatice și de comunicații; vor informa însă Centrul de comunicații și informatizare dacă un alt utilizator încearcă să obțină resurse pentru care nu este autorizat;

- utilizatorii nu vor rula programe care să expună sau să exploateze vulnerabilități ale sistemelor ce alcatuiesc resursele informatice și de comunicare (Exemple: programe de decriptare a parolilor, programe de captură de trafic, programe de scanare a rețelei);
- resursele informatice și de comunicații ce aparțin Institutului de Urgență pentru Boli Cardiovasculare și Transplant nu se vor folosi în scopuri personale;
- utilizatorii nu trebuie să acceseze, să creeze, să stocheze sau să transmită materiale pe care Institutul de Urgență pentru Boli Cardiovasculare și Transplant le poate considera ofensive, indecente sau obscene (altele decât cele în curs de cercetare academică unde acest aspect al cercetării are aprobarea explicită a conducerii Institutului);
- accesul la rețeaua Internet prin intermediul sistemelor ce compun resursele informatice și de comunicații se supune aceluiași regulamente care se aplică utilizării rețelei din interiorul instituției (Intranet);
- angajații nu trebuie să permită membrilor familiei sau altor persoane accesul la resursele informatice și de comunicații ale Institutului;
- utilizatorii nu trebuie să se angajeze în acțiuni împotriva intereselor /scopurilor Institutului de Urgență pentru Boli Cardiovasculare și Transplant folosind în acest scop resursele informatice și de comunicații;
- nu este permisă trimiterea sau recepționarea documentelor sau fișierelor care pot cauza acțiuni legale împotriva Institutului de Urgență pentru Boli Cardiovasculare și Transplant sau care prejudiciază interesele instituției;

Toate documentele, fișierele și mesajele - incluzând documentele, fișierele și mesajele personale - care sunt localizate în sistemul sau pe teritoriul Institutului de Urgență pentru Boli Cardiovasculare și Transplant sunt considerate proprietatea Institutului și pot fi subiectul unor cereri de verificare/inspectare/accesare conform regulamentelor.

Pentru buna gestionare, asigurarea confidențialității și protecției prelucrării datelor cu caracter personal privind starea de sănătate a pacienților internați sau monitorizați în ambulatoriul integrat al IBCvT Tg.Mures se adaugă în completarea regulilor sus-menționate :

- a) pentru studii clinice și contracte de cercetare/granturi , se utilizează modelele de consimțământ informat scris pentru prelucrarea datelor cu caracter personal privind starea de sănătate, specifice fiecărui proiect în parte, avizate de către Comisia Națională de Etică , respectiv Consiliul Etic al IBCvT Tg. Mureș și aprobate de conducerea acestuia;
- b) pentru activități de diagnostic și tratament medical, se utilizează modelele de consimțământ informat scris, specifice fiecărei secții clinice/ laborator, avizate de Consiliul Etic și aprobate de conducerea Institutului;
- c) pentru activitatea de învățământ-cercetare științifică medicală din IBCvT Tg.Mures se utilizează modelul de consimțământ informat avizat de Consiliul Etic și aprobat de conducerea Institutului, pus la dispoziție de directorul de cercetare-dezvoltare și/sau de directorul medical.

9. Măsuri sancționatorii

Încălcarea dispozițiilor impuse prin Politica de Securitate se sancționează prin măsuri disciplinare care pot include:

- Sancțiuni disciplinare pentru angajați conform prevederilor Codului Muncii;
- Notificarea și încetarea relațiilor contractuale (de colaborare) în cazul furnizorilor sau consultanților și recuperarea după caz, a prejudiciilor materiale și morale;
- Notificarea conducerii Universității de Medicină și Farmacie Târgu Mureș în cazul studenților precum și limitarea sau interzicerea accesului acestora la baza de date medicale din Secțiile clinice ale Institutului;

- Notificarea conducerii Direcției de Sănătate Pulică Mureș în cazul medicilor rezidenți precum și limitarea sau interzicerea accesului acestora la baza de date medicale din Secțiile clinice ale Institutului;

Toate acțiunile care contravin legilor în vigoare, în special cele privind prelucrarea datelor cu caracter personal, libera circulație a datelor și protecția vieții private vor fi raportate organelor competente.

10. Alte dispoziții

Prezenta Politică de Securitate are ca parte integrantă următoarele dispoziții:

- întreg personalul Institutului de Urgență pentru Boli Cardiovasculare și Transplant este responsabil privind aplicarea Politicii de Securitate și a modului de utilizare a resurselor informatice și de comunicații; fiecare utilizator este direct responsabil pentru acțiunile care pot afecta securitatea resurselor informatice și de comunicații sau imaginea instituției;
- utilizatorii sunt responsabili nediscriminatoriu privind raportarea oricărei suspiciuni sau confirmări de încălcare a prezentei Politici;
- Institutul nu va garanta confidențialitatea datelor personale ale angajaților aflate pe teritoriul său sau a accesului la informații folosind protocoale de genul, dar nu numai, mesagerie electronică personală, navigare Web, conversații telefonice, transmisie fax-uri și alte instrumente de conversație electronică. Utilizarea de către angajați pe teritoriul Institutului a acestor instrumente de comunicație poate fi monitorizată în scopul unor investigații sau al rezolvării unor plângeri în condițiile legilor în vigoare;
- conducerile Secțiilor clinice aparținând Institutului sunt responsabile de numirea și autorizarea utilizatorilor pentru folosirea adecvată a resurselor informatice și de comunicații;
- orice informație folosită în sistem trebuie să fie păstrată confidențială și în siguranță de către utilizator. Faptul că informațiile pot fi stocate electronic nu schimbă caracterul lor de secret de serviciu și secret profesional, fiind obligatorie păstrarea confidențialității și a siguranței. Tipul informației sau chiar informația în sine stau la baza determinării gradului de siguranță necesar;
- licențele software, aplicațiile și codul sursă al acestora, documentația și datele referitoare la echipamentele informatice trebuie protejate fiind proprietatea Institutului;
- secțiile clinice trebuie să ofere facilități corespunzătoare de control al accesului în scopul monitorizării resurselor informatice și de comunicații, protejării datelor și programelor împotriva întrebuințării greșite, în concordanță cu necesitățile stabilite de conducerile Secțiilor clinice. Accesul utilizatorilor trebuie să fie documentat, autorizat și controlat în mod corespunzător;
- orice software utilizat în cadrul Institutului trebuie să fie însoțit de licența care să specifice clar drepturile de utilizare și restricțiile produsului. Personalul trebuie să respecte prevederile licențelor și nu este permisă copierea ilegală a programelor. Centrul de comunicații și informatizare, direct sau prin intermediul reprezentantului Biroului IT, își rezervă dreptul de a șterge orice produs fără licență de pe orice sistem de calcul ce aparține sau este utilizat în interesul Institutului de Urgență pentru Boli Cardiovasculare și Transplant;
- Centrul de comunicații și informatizare, direct sau prin intermediul reprezentantului Biroului IT, își rezervă dreptul de a șterge orice program sau fișier care nu are legătură cu activitatea Institutului și este folosit în interes personal.

11. Dispoziții finale

- Politica de Securitate a Institutului de Urgență pentru Boli Cardiovasculare și Transplant impune dezvoltarea, gestionarea și punerea în practică de proceduri și/sau regulamente

specifice. Toate procedurile și/sau regulamentele de securitate a resurselor informatice și de comunicații fac parte din Planul de Securitate și sunt obligatorii pentru toți utilizatorii;

- Centrul de comunicații și informatizare are obligația de a revizui periodic prezenta Politică de Securitate și a propune conducerii Institutului dezvoltarea și modificarea Planului de Securitate;

- prevederile Politicii de Securitate vor fi incluse în contractele de muncă ale angajaților precum și în toate contractele cu terți (dacă activitatea acestora are legătură cu sistemul informatic și de comunicații al Institutului);

- componentele Planului de Securitate vor fi elaborate de către Centrul de comunicații și informatizare și vor fi propuse pentru aprobare conducerii Institutului de Urgență pentru Boli Cardiovasculare și Transplant Târgu Mureș;

- prezentul document și componentele Planului de Securitate vor conține informații de identificare proprii și se va specifica data la care acestea au fost aprobate și data de la care intră în vigoare;

- prezentul document și Planul de Securitate a sistemului resurselor informatice și de comunicații, nota de informare, modelele de consimțământ informat pentru activități medicale, respectiv de învățământ și cercetare, vor fi disponibile în format electronic pe sit-ul web al Institutului de Urgență pentru Boli Cardiovasculare și Transplant Târgu Mureș;

- modificarea prevederilor unei reguli sau proceduri din prezenta Politică de Securitate se va face numai cu aprobarea conducerii Institutului de Urgență pentru Boli Cardiovasculare și Transplant Târgu Mureș, sau prin efectul legii. Fiecare modificare a conținutului va conduce la modificarea versiunii documentului și a informațiilor de identificare. Versiunea anterioară rămâne valabilă până în momentul în care noua versiune intră în vigoare;

- Planul de securitate va conține o listă a tuturor regulamentelor și procedurilor aplicabile în sistemul resurselor informatice și de comunicații.

Observație:

*Orice persoană are dreptul de a se opune, pentru motive legitime, la prelucrarea datelor ce o privesc. Acest drept de opoziție poate fi exclus pentru anumite prelucrări prevăzute de lege (de ex.: prelucrări efectuate de serviciile financiare și fiscale, de poliție, justiție, securitate socială). Prin urmare, această mențiune nu poate figura dacă prelucrarea are un caracter obligatoriu; orice persoană are, de asemenea, dreptul de a se opune, în mod gratuit și fără nici o justificare, la prelucrările datelor sale personale în scopuri de marketing direct.

Refuzul oricărui pacient din IBCvT Tg. Mureș de a i se prelucra datele cu caracter personal privind starea sa de sănătate nu va trebui să afecteze calitatea îngrijirii și a tratamentului de care beneficiază din partea personalului medical

12. Referințe

- RFC 1244 – Site Security Handbook: <http://www.ietf.org/rfc/rfc1244.txt>;
- ISO 17799 – Standard detaliat de securitate;
- Legea nr. 676 din 21.11.2001 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul telecomunicațiilor;
- Legea nr. 677 din 21.11.2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date;
- Legea nr. 455 din 18.07.2001 privind semnătura electronică;
- Legea nr. 544 din 12.10.2001 privind liberul acces la informațiile de interes public;
- Hotărârea nr. 1259 din 13.12.2001 privind aprobarea Normelor tehnice și metodologice pentru aplicarea Legii nr. 455/2001 privind semnătura electronică;

- Ordinul nr. 52 din 18.04.2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal;
- Ordinul nr. 53 din 18.04.2002 privind aprobarea formularelor tipizate ale notificărilor prevăzute de Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date;
- Hotărârea nr. 781 din 25.07.2002 privind protecția informațiilor secrete de serviciu.
- Legea nr. 182 din 12.04.2002 privind protecția informațiilor clasificate;
- Legea nr. 161 din 19.04.2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției.