MINISTERUL TRANSPORTURILOR ŞI INFRASTRUCTURII

SPITALUL CLINIC CĂI FERATE IAŞI

Iaşi, Cod 700506, Str. Garabet Ibrăileanu, Nr. 1, C.I.F.: 4981239, E-mail: spitalcfiasi@yahoo.com
Tel.: 0232/216422 Secretariat Tel./Fax: 0232/264013 Web: www.spitaluniversitarcfiasi.ro

POLITICA DE SECURITATE PRIVIND SISTEMUL RESURSELOR INFORMATICE ŞI DE COMUNICAŢII PO STA-04

NOTĂ:

Acest document este proprietatea intelectuală a Spitalului Clinic Căi Ferate Iaşi.

Reproducerea integrală sau parţială a acestui document este permisă numai cu acordul prealabil scris şi înregistrat al managerului spitalului.

Constituie abatere disciplinara necunoaşterea şi/sau neaplicarea întocmai a cerinţelor prezentului document.

Aceasta abatere va fi sancţionată conform art. 247, 248 şi art. 250-252 din Codul Muncii, actualizat.

Revizie

Revizia acestui document se face ţinând cont de rezultatele implementării indicatorilor de monitorizare de structura, proces, rezultatelor obţinute, modificări legislative, modificări de circuite, reorganizări interne, etc.

Revizia nu este obligatorie decât dacă se îndeplinesc cel puţin unul dintre criteriile sus menţionate.

Situația ediției și a reviziilor în cadrul ediției procedurii

Nr crt	Ediția/ revizia în cadrul ediției	Componența revizuită	Modalitatea reviziei	Data la care se aplică prevederile ediției sau reviziei ediției
1	1/0	-integral	-elaborare inițială	15.01.2014
2	2/0	- integral	- modificare machetă procedură, actualizare lista responsabilități,actualizare legislație, actualizare descriere procedură	08.08.2022

Lista responsabililor cu elaborarea, verificarea și aprobarea ediției sau, după caz, a reviziei în cadrul ediției procedurii

Nr crt.	Elaborat / verificat / avizat / aprobat	Nume și prenume	Funcția	Semnatura	Data
1	**Elaborat**	Iulia Berbuncă	Statistician		18.07.2022
2	**Verificat**	Av. Petru MANIȚA	Avocat		20.07.2022
3	**Verificat**	Dr. Stela Maria LEONTE	Responsabil Managementul Calității		22.07.2022
4	**Avizat**	Dr. Izabela Lăcrămioara FRUNZĂ	Membru Comisiei de Monitorizare		26.07.2022
5	**Avizat**	Dr. Emilia SOLOMON	Director Medical		26.07.2022
6	**Aprobat**	Dr. Mihai GLOD	Manager		02.08.2022

SPITALUL CLINIC CF IAȘI ROMANIA

Exemplar nr.:

CUPRINS:

1. SCOP

Stabileşte obligatiile ce revin celor care au acces la resursele informatice si de comunicatii ale spitalului.

2. DOMENIUL DE APLICARE

Procedura se aplică la ***Spitalului Clinic Căi Ferate Iași*** în ***Compartimentul de evaluare și statistică medicală*** și în celelalte compartimente/birouri și secții ale spitalului.

3. DEFINIȚII ȘI ABREVIERI

3.1. Definiţii :

3.1.1. Administratorul Resurselor Informatice și de Comunicații (ARIC)= Responsabil la nivelul ***Spitalului Clinic Căi Ferate Iași*** cu administrarea şi finanţarea RIC ale ***Spitalului Clinic Căi Ferate Iași***. Desemnarea ARIC are ca scop stabilirea în mod clar a responsabilităţii privind crearea, modificarea şi aprobarea regulamentelor privind activităţile de finanţare, administrare şi utilizare a RIC. Dacă nu este desemnat un ARIC de către conducerea spitalului, titlul este atribuit în mod automat managerului ***Spitalului Clinic Căi Ferate Iași***

3.1.2 Ofiţer responsabil cu Securitatea RIC (OSRIC)= Răspunde în faţa ARIC privind administrarea funcţiilor de securitate a informaţiei în cadrul ***Spitalului Clinic Căi Ferate Iași.*** Este persoana de contact intern şi extern a ***Spitalului Clinic Căi Ferate Iași*** pentru orice problemă în legătură cu securitatea RIC. Funcţia OSRIC este asumată de către şeful Departamentului de Comunicaţii Digitale (D.C.D.). Şeful D.C.D. poate numi o altă persoană în funcţia de OSRIC, persoană care trebuie validată de către ARIC .

3.1.3 Ofiţer responsabil cu securitatea RIC la nivel Departamental: (OSRICD)=Persoana responsabilă de monitorizarea şi implementarea controalelor de securitate şi a procedurilor pentru sistemul RIC la nivelul unui Compartiment/Birou sau Secţii. Acesta este desemnat de către conducătorul Compartimentului/Secției şi validat de către OSRIC.

3.1.4 Utilizator= O persoană, o aplicaţie automatizată sau proces utilizator autorizat de către ***Spitalul Clinic Căi Ferate Iași*** în conformitate cu procedurile şi regulamentele în vigoare, să folosească RIC.
3.1.5 Abuz de privilegii = Orice acţiune întreprinsă în mod voit de un utilizator, care vine în contradicţie cu regulamentele ***Spitalului Clinic Căi Ferate Iași*** i/sau legile în vigoare, inclusiv cazul în care, din punct de vedere tehnic, nu se poate preveni înfăptuirea de către utilizator a acţiunii respective.
3.1.6 Furnizor = Persoană fizică/juridică care oferă bunuri sau servicii ***Spitalului Clinic Căi Ferate Iași*** în baza unui contract comercial sau de colaborare.

3.2. Abrevieri:

3.2.1	FOCG	= foaie de observaţie clinică generală
3.2.2	FSZ	= foaie pentru spitalizarea de zi
3.2.3	DRG	= Diagnosis Related Groups (a se înţelege aplicaţia informatică denumită astfel)
3.2.4	SMDPC	= Setul minim de date la nivel de pacient pentru spitalizare continuă
3.2.5	SMDPZ	= Setul minim de date la nivel de pacient pentru spitalizarea de zi
3.2.6	SIUI	= sistemul informatic unic integrat
3.2.7	MF	= medic de familie
3.2.8	CO	= concediu de odihnă
3.2.9	CM	= concediu medical
3.2.10	CNP	= cod numeric personal
3.2.11	Ed.	= Ediţie
3.2.12	Rev.	= Revizie
3.2.13	PO	= Procedură operaţională
3.2.14	RMC	= Responsabil cu sistemul de management al calităţii
3.2.15	CI	= Coordonator implementare
3.2.16	RC	= Reprezentantul conducerii cu sistemul de management al calităţii
3.2.17	PC	= Preşedintele comisiei
3.2.18	SCIM	= Sistem de control intern managerial
3.2.19	Comisie	= Comisia de monitorizare a dezvoltării sistemului de control intern managerial
3.2.20	Art.	= articol
3.2.21	Alin.	= Alineat
3.2.22	lit.	= Litera
3.2.23	SMI	= Sistem de Management Integrat (calitate, mediu, sănătate şi securitate ocupaţională)
3.2.24	ARIC	= Administratorul Resurselor Informatice şi de Comunicţii
3.2.25	OSRIC	= Ofiţer responsabil cu Securitatea RIC
3.2.26	OSRICD	= Ofiţer responsabil cu securitatea RIC la nivel Departamental

4. DOCUMENTE DE REFERINȚĂ

4.1. SR CEN/TS 15224:2017 - „Sisteme de management al calităţii. Aplicarea EN ISO 9001:2015 în îngrijirea sănătăţii"
4.2. SR EN ISO 9000:2015 – „Sisteme de management al calităţii. Principii fundamentale şi vocabular."
4.3. SR EN ISO 9001:2015 – „Sisteme de management al calităţii. Cerinţe."
4.4. Ordinul nr. 600/2018 - pentru aprobarea Codului controlului intern managerial al entităţilor publice
4.5. Legea 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal;
4.6. Ordinul 52/2002 privind aprobarea cerinţelor minime de securitate a prelucrărilor de date cu caracter personal;
4.7. Ordinul 53/2002 privind aprobarea formularelor tipizate ale notificărilor prevăzute de legea nr.677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal;
4.8. Legea nr. 455/2001 privind semnatura electronică.
4.9. Legea nr.544/2001 privind liberul acces la informaţiile de interes public.

4.10. Decizie de formare a Comisiei de monitorizare cu privire la sistemele de control intern managerial a ***Spitalului Clinic Căi Ferate Iași.***

4.11. Regulament de organizare şi de lucru al Comisiei de monitorizare a dezvoltării sistemului de control intern managerial al ***Spitalului Clinic Căi Ferate Iași***

5. DESCRIEREA PROCEDURII

5.1. Identificarea și autentificarea utilizatorului

Utilizatorii, pentru a căpata acces la o bază de date cu caracter personal, trebuie să se identifice. Identificarea se poate face prin: introducerea user-ului și a unei parole personale. Fiecare utilizator are propriul user și propria parolă. Niciodată mai mulți utilizatori nu trebuie să aibă același user. User-ele și parolele persoanelor care nu mai sunt angajați la ***Spitalul Clinic Căi Ferate Iași*** trebuie dezactivate imediat ce inginerului de sistem i-au fost comunicate datele despre persoana în cauză. Parolele sunt șiruri de caractere. Cu cât șirul de caractere este mai lung, cu atât parola este mai greu de aflat. La introducerea parolelor acestea nu sunt afisate în clar pe monitor. Schimbarea periodică a parolelor se poate face numai de către utilizatori din meniul intern aplicației informatice. În aplicațiile DRG și SIUI parola se poate schimba la soliciarea utilizatorului făcută către persoana responsabilă în domeniul IT.
Orice utilizator care primește un user și o parolă trebuie să păstreze confidențialitatea acestora și să răspundă în acest sens în fața conducerii.

5.2. Accesul utilizatorului

Utilizatorii aplicațiilor pot accesa numai anumite tipuri de date în funcție de natura responsabilității sale, drepturile sunt acordate pe funcționalitate (cum ar fi: administrare, introducere, prelucrare, salvare, trimitere analize, tipărire, cerere rapoarte etc.) și după acțiuni aplicate asupra datelor cu caracter personal (cum ar fi: scriere, citire, ștergere).

5.3. Colectarea datelor

Orice modificare a datelor cu caracter personal se poate face numai de către utilizatori autorizați.
S-au luat măsuri pentru ca sistemul informațional să înregistreze cine a făcut modificarea, data și ora modificării.

5.4. Execuția copiilor de siguranță

Intervalul de timp la care se vor executa copiile de siguranță ale bazelor de date cu caracter personal, precum și ale programelor folosite pentru prelucrările automatizate este de 1 lună calendaristică după ce s-au făcut raportările. Singura persoana autorizată să facă copii de siguranță este persoana responsabilă în domeniul IT. Copiile de siguranță se vor da la pavilionul administrativ (clădire monitorizată video) în casierie, într-un seif.

5.5. Computerele și terminalele de acces

Serverul aplicației informatice se află în pavilionul Administrativ clădire care este monitorizată video în permananță, într-o cameră tehnică încuiată special dedicată acestui terminal. Serverul se află și într-un rack metalic încuiat. Accesul (cheile) la serverul aplicației informatice îl are doar persoana responsabilă în domeniul IT. Serverul aplicației informatice este în permanență parolat.
Serverul aplicației SIUI și calculatorul pe care se face raportarea DRG se găsește în pavilionul administrativ la Compartimentul Statistică. Biroul este încuiat cu cheie, are gratii la geam iar terminalele au parola de acces. Accesul la Compartimentul Statistică îl au persoana responsabilă în domeniul IT, statisticianul și operatorul de date.
Calculatoarele care conțin date cu caracter personal au funcție de temporizare iar după 1 minut intră în screen saver-ul cu funcția de log-on activată. Deci utilizatorii vor trebui să se autentifice iar.
La aplicația informatică pe ecran apar date cu caracter personal. Dacă asupra lor nu se acționează o perioadă mai mare de 5 minute, sesiunea de lucru se închide automat.

Calculatoarele de acces folosite în relația cu publicul, pe care apar date cu caracter personal, sunt poziționate astfel încât datele de pe ecran să nu poată fi văzute de public ți dupa o perioadă de 1 minut de inactivitate intră automat screen saver cu funcția de logare. Aplicația informatică își închide sesiunea de lucru după un interval de inactivitate de 5 minute.

5.6. Fișierele de acces

Operatorul este obligat să ia măsuri ca orice accesare a bazei de date cu caracter personal să fie înregistrată într-un fisier de acces (numit log la prelucrările automate) sau într-un registru pentru prelucrările manuale de date cu caracter personal, stabilit de operator. Informațiile înregistrate în fișierul de acces sau în registru vor fi:

- codul de identificare (numele utilizatorului pentru bazele de date cu caracter personal manuale);
- numele fișierului accesat (fișei);
- numărul înregistrărilor efectuate;
- tipul de acces;
- codul operației executate sau programul folosit;
- data accesului (an, luna, zi);
- timpul (ora, minutul, secunda).

Pentru prelucrările automate aceste informații vor fi stocate într-un fișier de acces general sau în fișiere separate pentru fiecare utilizator. Orice încercare de acces neautorizat va fi, de asemenea, înregistrată. Operatorul este obligat să păstreze fișierele de acces cel puțin 2 ani, pentru a fi folosite ca probe în cazul unor investigații. Dacă investigațiile se prelungesc, aceste fișiere se vor păstra atât timp cât se va considera necesar. Fișierele de acces trebuie să facă posibilă identificarea de către operator sau de către persoana imputernicită a persoanelor care au accesat date cu caracter personal fără un motiv anume, în vederea aplicării unor sancțiuni sau a sesizării organelor competente.

5.7. Sistemele de telecomunicații

Comunicația Server-Stații de lucru se realizează prin fibra optică și VPN la nivel de oraș pentru locațiile exterioare. Pe fiecare locație comunicația se face prin fibra optică, cablu ftp sau utp. La unele locații din cauza particularităților clădirii comunicația cu stațiile de lucru se face criptată și parolată prin wireless. Filtrarea și autentificarea se face pe baza ip-ului și a mac-ului plăcii de rețea astfel se evită accesul neautorizat în rețea.

5.8. Instruirea personalului

In cadrul cursurîlor de pregătire a utilizatorilor s-a făcut informarea acestora cu privire la prevederile Legii pentru protectia persoanelor cu privire la prelucrarea datelor cu caracter personal și liberă circulație a acestor date, la cerințele minime de securitate a prelucrărilor de date cu caracter personal, precum și cu privire la riscurile pe care le comporta prelucrarea datelor cu caracter personal, în funcție de specificul activității utilizatorului. Utilizatorii care au acces la date cu caracter personal au fost instruiți asupra confidentialității .Utilizatorii sunt obligați să își închidă sesiunea de lucru atunci când părăsesc locul de muncă.

5.9. Folosirea computerelor

Pentru menținerea securității prelucrării datelor cu caracter personal (în special împotriva virusilor informatici) persoana responsabilă în domeniul IT va lua măsuri care vor consta în:
a)interzicerea folosirii de către utilizatori a programelor software care provin din surse externe sau dubioase;
b)informarea utilizatorilor în privința pericolului privind virușii informatici;
c)implementarea unor sisteme automate de devirusare și de securitate a sistemelor informatice care sunt confidențiale și care nu pot fi prezentate din motive de securitate;

d)nu s-a facut dezactivarea tastei "Print screen", deoarece atunci când sunt afisate pe monitor date cu caracter personal utilizatorii autorizați au dreptul să printeze documentele dar numai în scopul strict al interesului de serviciu. Utilizatorii autorizați știu ca au obligația să închidă sesiunea de lucru din aplicații la parăsirea calculatorului.

5.10. Imprimarea datelor

Tipărirea la imprimantă a datelor cu caracter personal se va realiza numai de utilizatori autorizați pentru aceasta operațiune și doar în interes de serviciu.

6. RESPONSABILITĂȚI:

6.1. Responsabilități ale utilizatorilor resurselor informatice și de comunicații:

- Utilizatorii pot accesa aplicația informatică, SIUI sau DRG **numai** pe baza unui user-ul și parola acordate de persoana responsabilă în domeniul IT
- prelucrarea datelor se va face numai de către utilizatori desemnați;
- utilizatorii desemnați vor accesa datele cu caracter personal numai în interes de serviciu;
- operatorii care au acces la date cu caracter personal au obligația de păstra confidențialitatea acestora ;

se interzice folosirea de către utilizatori a programelor software care provin din surse externe sau dubioase, existând riscul ca odată cu accesarea acestor programe să pătrundă în sistem viruși informatici ce pot distruge bazele de date existente; se interzice descărcarea de pe internet a altor programe decât cele instalate de personalul din cadrul ***Compartimentului de evaluare și statistică medicală***.

- a fișierelor cu muzică, filme, poze etc;
- în programul informatic, SIUI sau DRG, persoanele desemnate pot accesa doar datele secției sau cabinetului unde lucrează sau în funcție de drepturile care i-au fost acordate în aplicații de către Persoana responsabilă în domeniul IT pot accesa și alte departamente, raportări etc.;

- se interzice ștergerea sau modificarea unor înregistrări din bazele de date; erorile de operare ce trebuie remediate, ori disfuncționalitățile din programul SIUI vor fi aduse la cunoștință în cadrul ***Compartimentului de evaluare și statistică medicală.***
- operatorii sunt obligați să își închidă sesiunea de lucru atunci când părăsesc locul de muncă;
- încăperile unde sunt amplasate calculatoarele trebuie să fie încuiate atunci când nu se află nimeni acolo;
- utilizatorul care primește un user și o parolă de autentificare trebuie să păstreze confidențialitatea acestora;

Încălcarea acestor dispoziții se vor aduce la cunoștință conducerii Spitalului ***Clinic Căi Ferate Iași*** astfel se vor decide măsurile ce trebuie luate, interzicerea accesului la sistemul informatic sau chiar posibilitatea rezilierii contractului de muncă.

6.2. Responsabilități ale persoanei desemnate responsabile cu programul DRG:

Persoana care a fost desemnată responsabilă cu programul DRG, are urmatoarele obligații (Operatorul de date):

- coordonează activitatea de introducere și validare date în programul DRG;
- colaborează permanent cu persoanele desemnate ca utilizatori ai programului informatic pe secție ;
- raportează Managerului toate problemele întâmpinate în procesul de introducere-validare date în programul DRG;
- se asigură ca prelucrarea datelor în programul DRG se face corect, că respectă politica ***Spitalului Clinic Căi Ferate Iași*** referitoare la securitatea prelucrării datelor cu caracter personal și raportează Managerului toate abaterile de la aceasta;
- are în vedere ca datele să fie introduse în program corect și la timp, astfel încât să se poată face raportările către SNSPMS la termen;

- răspunde în Managerului de corectitudinea înregistrărilor în program, de respectarea termenelor de raportare și a politicii de securitate a prelucrării datelor cu caracter personal.

6.3. Obligațiile persoanelor desemnate responsabile cu programul SIUI pe secții sau ambulatorii :
Persoanele care au fost desemnate responsabile cu programul SIUI pe secții sau ambulatorii, au urmatoarele obligații (Operatorul de date, Statisticianul și Registratorul medical):
- coordonează activitatea de introducere și validare date în programul SIUI pe secții sau ambulatorii;
- colaborează permanent cu persoanele desemnate ca utilizatori ai programului SIUI pe secție sau ambulatoriu;
- raportează inginerului de sistem toate problemele întâmpinate în procesul de introducere-validare date în programul SIUI;
- se asigură că prelucrarea datelor în programul SIUI se face doar de către utilizatorii desemnați, ca aceștia respectă politica ***Spitalului Clinic Căi Ferate Iași*** referitoare la securitatea prelucrării datelor cu caracter personal și raportează inginerului de sistem toate abaterile de la aceasta;
- are în vedere ca datele să fie introduse în program corect și la timp, astfel încât să se poată face raportările către CAS la termen;
- răspunde în fața conducerii spitalului de corectitudinea înregistrărilor în program, de respectarea termenelor de raportare și a politicii de securitate a prelucrării datelor cu caracter personal.

6.4. Obligațiile persoanei desemnată responsabil cu programul informatic**:**
Persoana desemnată responsabil cu buna funcționare are urmatoarele obligații (Persoana responsabilă în domeniul IT):
- coordonează activitatea de introducere și validare date în programul informatic ;
- asigură confidențialitatea datelor;
- colaborează cu firma de specialitate IT care asigură asistența tehnică de specialitate, căreia îi raportează toate disfuncționalitățile;
- solicită firmei IT realizarea unor copii de siguranță ale bazelor de date și asigură arhivarea acestora;
- răspunde de respectarea termenelor de raportare a situațiilor către **CAS**.
-răspunde în fața conducerii spitalului de corectitudinea înregistrărilor în program, de respectarea termenelor de raportare și a politicii de securitate a prelucrării datelor cu caracter personal.

7. EVIDENȚE ȘI ÎNREGISTRĂRI
-Lista utilizatorilor bazei de date informatică;
-Lista utilizatorilor bazei de date DRG;
-Lista utilizatorilor bazei de date SIUI;
-Lista responsabililor cu baza de date informatică;
-Lista responsabililor cu baza de date DRG;
-Lista responsabililor cu baza de date SIUI.

8. ANEXE
- Nu se aplică

9. DIFUZARE
Procedura se difuzează pe baza Listei de difuzare, cod PS 01/F3 sau în format electronic.
Înregistrările generate de această activitate se păstrează / arhivează conform cerințelor SMC/SCIM implementat.

10. INDICATORI DE MONITORIZARE

INDICATOR	TINTA	METODA DE CALCUL	PERIOADA DE MONITORIZARE	RESPONSABIL
Ponderea actualității documentelor de referință care stau la baza elaborarii procedurii .	100%	Nr documente de referință în actualitate / Nr total documente de referință.	Semestrial	Statistician
Ponderea angajaților instruiți cu cerințele procedurii din totalul angajaților cu atribuții în aplicarea cerințelor procedurii.	100%	Nr personal instruit cu cerințele procedurii / Nr angajaților cu atribuții în aplicarea cerințelor procedurii	Semestrial	Statistician
Ponderea incidentelor de securitate.	0	Nr incidente de securitate / 0	Semestrial	Statistician
Procent unități de lucru la care accesul se face pe bază de parolă din totalul unităților de lucru.	100%	Nr unități de lucru la care accesul se face pe baza de parola /Nr total unități de lucru	Semestrial	Statistician