1. Lista responsabililor cu elaborarea, verificarea şi aprobarea ediţiei sau, după caz, a reviziei în cadrul ediţiei procedurii de sistem

Nr. crt.	Elemente privind responsabilii operaţiunea	Numele şi prenumele	Funcţia	Data	Semnătura
	1	2	3	4	5
1.	Elaborat	Hegyi Pop Diana Adela	Registrator Medical	02.12.2020	
2.	Verificat		SMC		
3.	Avizat	SzutorZsigmond	Presedinte SCIM	02.12.2020	
4.	Aprobat	Kanya Botond	Manager	02.12.2020	

2. Situaţia ediţiilor şi a reviziilor în cadrul ediţiilor procedurii

Nr. crt.	Ediţia / Revizia în cadrul ediţiei	Componenta revizuită	Modalitatea reviziei	Data de la care se aplică prevederile ediţiei sau reviziei ediţiei
	1	2	3	4
1.	Ediţia 1 / Revizia 0	- integral	- elaborare iniţială	02.12.2020
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				

3.Scopul

3.1. Prezenta procedura stabileşte obligatiile ce revin celor care au acces la resursele informatice si de comunicatii ale spitalului.

4.Domeniul de aplicare

4.1. Procedura se aplică de către personalul compartimentului de statistica din cadrul Spitalului Orăşenesc Sângeorgiu De Pădure.

5.Documente de referinţă

5.1.SR EN ISO 9001:2015 „Sisteme de management al calităţii.Principii fundamentale şi vocabular. Cerinţe."

5.2. Ordin 600/2018, privind aprobarea codului Controlului intern managerial al entitatilor publice;

5.3. Ordinul MS nr.972/2010, privind aprobarea standardelor de acreditare

5.4. Ordinul nr. 1.782/2006 privind înregistrarea si raportarea statistică a pacienţilor care primesc servicii medicale în regim de spitalizare continuă si spitalizare de zi

5.5. Legea nr.46/2003, privind drepturile pacienutlui

5.6. O 440/2003 privind inregistrarea si raportarea statistica a pacientilor care primesc servicii medicale in regim de spitalizare de zi – Modificat de O 3/2004

5.7. O 29/2003 privind introducerea colectarii electronice a Setului minim de date la nivel de pacient (SMDP) in spitalele din Romania – Modificat de O 1623/2004

5.8. Ordinul 19/2011 privind completarea formularelor de raportare (codificarea categoriilor de asigurati)

5.9. Contract-Cadru privind conditiile acordarii asistentei medicale in cadrul sistemului de asigurari sociale de sanatate pentru anii 2013-2014

5.10. Ordinul 798/2002 privind introducerea in spitale a formularului FOAIA DE OBSERVATIE CLINICA GENERALA (Modificat de Ordinul 88/2004, Ordinul 798-1/2002 Anexa, Ordinul 798-2/2002 Instructiuni)

5.11. Ordinul nr.384/413/26.03.2009 privind aprobarea modelului unic al biletului de trimitere pentru servicii medicale

5.12. Ordin 617/2007 (MO 649/2007) cu modificarile si completarile ulterioare – Ordin pentru aprobarea Normelor metodologice privind stabilirea documentelor justificative pentru dobandirea calitatii de asigurat, respectiv asigurat fara plata contributiei, precum si pentru aplicarea masurilor de executare silita pentru incasarea sumelor datorate la Fondul national unic.

5.13. ORDIN Nr. 225/29.04.2013 - pentru aprobarea documentelor justificative privind raportarea activitatii realizate de catre furnizorii de servicii medicale - formulare unice pe tara, fara regim special

5.14. ORDIN nr. 226 din 29 aprilie 2013 - privind aprobarea Regulilor de validare a cazurilor spitalizate in regim de spitalizare continua si a Metodologiei de evaluare a cazurilor invalidate pentru care se solicita revalidarea

5.15. ORDIN Nr.423-191 din Martie 2013 - privind Normele metodologice de aplicare in anul 2013 a Contractului-cadru

5.16. ORDIN nr. 6 din 9 ianuarie 2013 pentru completarea Ordinului presedintelui Casei Nationale de Asigurari de Sanatate nr. 25/2012 privind aprobarea Regulilor de validare a cazurilor spitalizate in regim de spitalizare continua si a Metodologiei de evaluare a cazurilor invalidate pentru care se solicita revalidarea

5.17. Regulamentul (UE) 2016/679 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor),

5.18. Directiva (UE) 2016/680 referitoare la protecţia datelor personale în cadrul activităţilor specifice desfăşurate de autorităţile de aplicare a legii.

5.19. Legea nr. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor)
5.20. Decizie pentru numirea Comisiei pentru monitorizare, coordonare şi îndrumare metodologică a dezvoltării sistemului de control managerial al Spitalului Orășenesc Sângeorgiu De Pădure.
5.21. Regulament de organizare şi de lucru al Comisiei pentru monitorizare, coordonare şi îndrumare metodologică a
dezvoltării sistemului de control managerial al Spitalului Orășenesc Sângeorgiu De Pădure.

6. Definiţiişi abrevieri

6.1.Definiţii

Nr.crt.	Termenul	Definitia si/sau, dacă este cazul, actul care defineste termenul
1.	Nu este cazul	-

6.2.Abrevieri

Nr.crt.	Abrevierea	Termenul abreviat
1.	PO	Procedura operationala
2.	CM	Comisia de monitorizare, coordonare şi îndrumare metodologică a dezvoltării sistemului de control managerial al Spitalului
3.	SMC	Sistem management caliatate
4.	STAT	STATISTICA
5.	DRG	Diagnosis Related Groups
6.	SNSPMS	Scola Nationala de Sanatate Publica si Management Sanitar
7.	ICM	Indicele de complexitate al cazului

7.Descrierea procedurii

7.1.Identificarea si autentificarea utilizatorului

Utilizatorii, pentru a capata acces la o baza de date cu caracter personal, trebuie sa se identifice. Identificarea se poate face prin mai multe metode, cum ar fi: introducerea codului de identificare de la tastatura (un sir de caractere), folosirea unei cartele cu cod de bare, folosirea unei cartele inteligente (smart card) sau a unei cartele magnetice. Fiecare utilizator are propriul sau cod de identificare. Niciodata mai multi utilizatori nu trebuie sa aiba acelasi cod de identificare. Codurile de identificare (sau conturi de utilizator) nefolosite o perioada mai indelungata trebuie dezactivate si distruse dupa un control prealabil intern al operatorului. Perioada dupa care codurile trebuie dezactivate si distruse se stabileste de operator. Orice cont de utilizator este insotit de o modalitate de autentificare. Autentificarea poate fi facuta prin introducerea unei parole sau prin mijloace biometrice: amprenta dactiloscopica, amprenta vocala, angiografia retiniana etc. Parolele sunt siruri de caractere. Cu cat sirul de caractere este mai lung, cu atat parola este mai greu de aflat. La introducerea parolelor acestea nu trebuie sa fie afisate in clar pe monitor. Parolele trebuie schimbate periodic in functie de politicile de securitate ale entitatii (operator sau persoana imputernicita). Schimbarea periodica a parolelor se face numai de catre utilizatori autorizati de operator. Operatorul trebuie sa solicite realizarea unui sistem informational care

sa refuze automat accesul unui utilizator dupa 5 introduceri gresite ale parolei. Orice utilizator care primeste un cod de identificare si un mijloc de autentificare trebuie sa pastreze confidentialitatea acestora si sa raspunda in acest sens in fata opera-torului. Fiecare entitate va stabili o procedura proprie de administrare si gestionare a conturilor de utilizator. Operatorii autorizeaza anumiti utilizatori pentru a revoca sau a suspenda un cod de identificare si autentificare, daca utilizatorul acestora si-a dat demisia ori a fost concediat, si-a incheiat contractul, a fost transferat la alt serviciu si noile sarcini nu ii solicita accesul la date cu caracter personal, a abuzat de codurile primite sau daca va absenta o perioada indelungata stabilita de entitate. Accesul utilizatorilor la bazele de date cu caracter personal efectuate manual se va face pe baza unei liste apro-bate de conducerea entitatii.

7.2.Tipul de acces

Utilizatorii trebuie sa acceseze numai datele cu caracter personal necesare pentru indeplinirea atributiilor lor de serviciu. Pentru aceasta operatorii trebuie sa stabileasca tipurile de acces dupa functionalitate (cum ar fi: administrare, introducere, prelucrare, salvare etc.) si dupa actiuni aplicate asupra datelor cu caracter personal (cum ar fi: scriere, citire, stergere), precum si procedurile privind aceste tipuri de acces. Programatorii sistemelor de prelucrare a datelor cu caracter personal nu vor avea acces la datele cu caracter personal. Operatorul va permite accesul programatorilor la datele cu caracter personal dupa ce acestea au fost transformate in date anonime. Compartimentul care asigura suportul tehnic poate avea acces la datele cu caracter personal pentru rezolvarea unor cazuri exceptionale. Pentru activitatea de pregatire a utilizatorilor sau pentru realizarea de prezentari se vor folosi date anonime. Angajatii care predau cursurile de pregatire vor folosi date cu caracter personal pe parcursul propriei lor pregatiri. Operatorul va stabili modalitatile stricte prin care se vor distruge datele cu caracter personal. Autorizarea pentru aceasta prelucrare de date cu caracter personal trebuie limitata la cativa utilizatori.

7.3.Colectarea datelor

Operatorul desemneaza utilizatori autorizati pentru operatiile de colectare si introducere de date cu caracter personal intr-un sistem informational. Orice modificare a datelor cu caracter personal se poate face numai de catre utilizatori autorizati desemnati de operator. Operatorul va lua masuri pentru ca sistemul informational sa inregistreze cine a facut modificarea, data si ora modificarii. Pentru o mai buna administrare operatorul va lua masuri ca sistemul informational sa mentina datele sterse sau modificate.

7.4.Executia copiilor de siguranta

Operatorul va stabili intervalul de timp la care se vor executa copiile de siguranta ale bazelor de date cu caracter personal, precum si ale programelor folosite pentru prelucrarile automatizate. Utilizatorii care executa aceste copii de siguranta vor fi numiti de operator, intr-un numar restrans. Copiile de siguranta se vor stoca in alte camere, in fisete metalice cu sigiliu aplicat, si, daca este posibil, chiar in camere din alta cladire. Operatorul va lua masuri ca accesul la copiile de siguranta sa fie monitorizat.

7.5.Computerele si terminalele de acces

Computerele si alte terminale de acces vor fi instalate in incaperi cu acces restrictionat. Daca nu pot fi asigurate aceste conditii, computerele se vor instala in incaperi care se pot incuia sau se vor lua masuri ca accesul la computere sa se faca cu ajutorul unor chei ori cartele magnetice. Daca pe ecran apar date cu caracter personal asupra carora nu se actioneaza o perioada data, stabilita de operator, sesiunea de lucru trebuie inchisa automat. Marimea acestei perioade se determina in functie de operatiile care trebuie executate. Terminalele de acces folosite in relatia cu publicul, pe care apar date cu caracter personal, vor fi pozitionate astfel incat sa nu poata fi vazute de public si dupa o perioada scurta, stabilita de operator, in care nu se actioneaza asupra lor, acestea trebuie ascunse.

7.6.Fisierele de acces

Operatorul este obligat sa ia masuri ca orice accesare a bazei de date cu caracter personal sa fie inregistrata intr-un fisier de acces (numit log la prelucrarile automate) sau intr-un registru pentru prelucrarile manuale de date cu caracter personal, stabilit de operator. Informatiile inregistrate in fisierul de acces sau in registru vor fi:

- codul de identificare (numele utilizatorului pentru bazele de date cu caracter personal manuale);
- numele fisierului accesat (fisei);
- numarul inregistrarilor efectuate;
- tipul de acces;
- codul operatiei executate sau programul folosit;
- data accesului (an, luna, zi);
- timpul (ora, minutul, secunda).

Pentru prelucrarile automate aceste informatii vor fi stocate intr-un fisier de acces general sau in fisiere separate pentru fiecare utilizator. Orice incercare de acces neautorizat va fi, de asemenea, inregistrata. Operatorul este obligat sa pastreze fisierele de acces cel putin 2 ani, pentru a fi folosite ca probe in cazul unor investigatii. Daca investigatiile se prelungesc, aceste fisiere se vor pastra atat timp cat se va considera necesar. Fisierele de acces trebuie sa faca posibila identificarea de catre operator sau de catre persoana imputernicita a persoanelor care au accesat date cu caracter personal fara un motiv anume, in vederea aplicarii unor sanctiuni sau a sesizarii organelor competente.

7.7.Sistemele de telecomunicatii

Operatorul este obligat sa faca periodic controlul autentificarilor si tipurilor de acces pentru detectarea unor disfunctionalitati in ceea ce priveste folosirea sistemelor de telecomunicatii. Operatorii sunt obligati sa conceapa sistemul de telecomunicatii astfel incat datele cu caracter personal sa nu poata fi interceptate sau transmise de oriunde. Daca sistemul de telecomunicatii nu poate fi astfel securizat, operatorul este obligat sa impuna folosirea metodei de criptare pentru transmisia datelor cu caracter personal. Prin sistemele de telecomunicatii se vor transmite numai datele cu caracter personal strict necesare.

7.8.Instruirea personalului

In cadrul cursurilor de pregatire a utilizatorilor operatorul este obligat sa faca informarea acestora cu privire la Regulamentul (UE) 2016/679 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor), la cerintele minime de securitate a prelucrarilor de date cu caracter personal, precum si cu privire la riscurile pe care le comporta prelucrarea datelor cu caracter personal, in functie de specificul activitatii utilizatorului. Utilizatorii care au acces la date cu caracter personal vor fi instruiti de catre operator asupra confidentialitatii acestora si vor fi avertizati prin mesaje care vor aparea pe monitoare in timpul activitatii. Utilizatorii sunt obligati sa isi inchida sesiunea de lucru atunci cand parasesc locul de munca.

7.9.Folosirea computerelor

Pentru mentinerea securitatii prelucrarii datelor cu caracter personal (in special impotriva virusilor informatici) operatorul va lua masuri care vor consta in:

a)interzicerea folosirii de catre utilizatori a programelor software care provin din surse externe sau dubioase;

b)informarea utilizatorilor in privinta pericolului privind virusii informatici;

c)implementarea unor sisteme automate de devirusare si de securitate a sistemelor informatice;

d)dezactivarea, pe cat posibil, a tastei "Print screen", atunci cand sunt afisate pe monitor date cu caracter personal, interzicandu-se astfel scoaterea la imprimanta a acestora.

7.10. Imprimarea datelor

Scoaterea la imprimanta a datelor cu caracter personal se va realiza numai de utilizatori autorizati pentru aceasta operatiune de catre operator. Operatorii sunt obligati sa aprobe proceduri interne specifice privind folosirea si distrugerea acestor materiale. Fiecare entitate isi va aproba propriul sistem de securitate, tinand seama de aceste cerinte minime de securitate a prelucrarilor de date cu caracter personal, iar in functie de importanta datelor cu caracter personal prelucrate, isi va impune masuri de securitate suplimentare.

8.Responsabilităţi:

8.1.Responsabilitati ale utilizatorilor resurselor informatice si de comunicatii:

- prelucrarea datelor se va face numai de catre utilizatori desemnati ;
- utilizatorii desemnati vor accesa datele cu caracter personal numai in interes de serviciu;
- operatorii care au acces la date cu caracter personal au obligatia de pastra confidentialitatea acestora ;
- se interzice folosirea de catre utilizatori a programelor software care provin din surse externe sau dubioase, existand riscul ca odata cu accesarea acestor programe sa patrunda in sistem virusi informatici ce pot distruge bazele de date existente; se interzice descarcarea de pe internet a altor programe decat cele instalate de personalul **Comp.Statistica Medicala**, a fisierelor cu muzica, filme, poze etc;
- in programul ICEMED (SIUI), persoanele desemnate vor accessa doar datele sectiei sau cabinetului unde lucreaza, pentru a evita disfunctionalitatea programului;
- se interzice stergerea sau modificarea unor inregistrari din bazele de date; erorile de operare ce trebuie remediate, ori disfunctionalitatile din programul ICEMED (SIUI) vor fi aduse la cunostinta **Comp.Statistica Medicala** ;
- operatorii sunt obligati sa isi inchida sesiunea de lucru atunci cand parasesc locul de munca;
- incaperile unde sunt amplasate calculatoarele trebuie sa fie incuiate atunci cand nu se afla nimeni acolo;
- terminalele de acces folosite vor fi pozitionate astfel incat sa nu poata fi vazute de public;
- utilizatorul care primeste un cod de identificare si un mijloc de autentificare trebuie sa pastreze confidentialitatea acestora;

incalcarea acestor dispozitii va duce la interzicerea accesului la sistemul informatic sau chiar la rezilierea contractului de munca.

8.2.Responsabilitati ale persoanelor desemnate responsabile cu programul ICEMED:

Persoanele care au fost desemnate responsabile cu programul ICEMED au urmatoarele obligatii:

- coordoneaza activitatea de introducere si validare date in program;
- raporteaza responsabilului cu baza de date DRG pe spital toate problemele intampinate in procesul de introducere-validare date in programul DRG;
- se asigura ca prelucrarea datelor in programul DRG se face doar de catre utilizatorii desemnati, ca acestia respecta politica ***Spitalului Orășenesc Sângeorgiu De Pădure*** referitoare la securitatea prelucrarii datelor cu caracter personal si raporteaza responsabilului cu baza de date DRG pe spital toate abaterile de la aceasta;
- are in vedere ca datele sa fie introduse in program corect si la timp, astfel incat sa se poata face raportarile catre SNSPMS la termen;

- raspunde in fata responsabilului cu baza da date pe spital si a conducerii spitalului de corectitudinea inregistrarilor in program, de respectarea termenelor de raportare si a politicii de securitate a prelucrarii datelor cu caracter personal.

8.3.Obligatiile persoanelor desemnate responsabile cu programul ICEMED (SIUI)
Persoanele care au fost desemnate responsabile cu programul ICEMED(SIUI) pe spital, au urmatoarele obligatii:
- coordoneaza activitatea de introducere si validare date in programul SIUI ;
- colaboreaza permanent cu persoanele desemnate ca utilizatori ai programului SIUI;
- raporteaza responsabilului cu baza de date SIUI pe spital toate problemele intampinate in procesul de introducere-validare date in programul SIUI;
- se asigura ca prelucrarea datelor in programul SIUI se face doar de catre utilizatorii desemnati, ca acestia respecta politica ***Spitalului Orășenesc Sângeorgiu De Pădure*** referitoare la securitatea prelucrarii datelor cu caracter personal si raporteaza responsabilului cu baza de date SIUI pe spital toate abaterile de la aceasta;
- are in vedere ca datele sa fie introduse in program corect si la timp, astfel incat sa se poata face raportarile catre CAS la termen;
- raspunde in fata responsabilului cu baza da date SIUI pe spital si a conducerii spitalului de corectitudinea inregistrarilor in program, de respectarea termenelor de raportare si a politicii de securitate a prelucrarii datelor cu caracter personal.

8.4.Obligatiile persoanei desemnata responsabil cu baza de date din farmacia spitalului:
Persoana desemnata responsabil cu baza de date din farmacia spitalului are urmatoarele obligatii:
- coordoneaza activitatea de introducere si validare date;
- asigura confidentialitatea datelor;
- raspunde de respectarea termenelor de raportare a situatiilor catre CAS.
- raspunde in fata conducerii spitalului de corectitudinea inregistrarilor in program, de respectarea termenelor de raportare si a politicii de securitate a prelucrarii datelor cu caracter personal.

9.Anexe, înregistrări, arhivări
9.1. Anexa – nu este cazul
9.2. Inregistrari :
-Lista utilizatorilor bazei de date DRG;
-Lista utilizatorilor bazei de date SIUI;
-Lista responsabililor cu baza de date DRG;
-Lista responsabililor cu baza de date SIUI.
-Persoana desemnata responsabila cu baza de date din farmacie

10. DIFUZARE
Procedura este pusă la dispoziţia utilizatorilor de Secretariat Tehnic pe suport informatic şi pe suport hârtie.
Înregistrările generate de această activitate se păstrează/arhivează conform cerinţelor SCIM implementat