



**SPITALUL DE PSIHIATRIE VOILA**  
Mun. Campina, str. Voila nr. 114, jud. Prahova  
TEL: 0244 / 335 161; FAX: 0344-102034  
E-mail: [spitalpsihiatrie@clicknet.ro](mailto:spitalpsihiatrie@clicknet.ro); Web: [www.spitalulvoila.ro](http://www.spitalulvoila.ro)  
Nr. 3688/29.05.2015

---

**APROBAT MANAGER INTERIMAR**  
**DR. IRINA MINESCU**



**POLITICA DE SECURITATE**  
**A PRELURARILOR DE DATE CU CARACTER PERSONAL**

**1. Angajamentul Spitalului de Psihiatrie Voila:**

Protejarea sigurantei si securitatii datelor cu caracter personal este importanta pentru Spitalul de Psihiatrie Voila, prin urmare activitatile desfasurate de noi sunt in conformitate cu legislatia aplicabila referitoare la protectia sigurantei datelor si la securitatea acestora.

Accesand pagina noastra de internet ([www.spitalulvoila.ro](http://www.spitalulvoila.ro)), veti lua la cunostinta asupra "Notei de informare privind protectia datelor personale".

**2. Scopul documentului:** prezentul document reglementeaza măsurile tehnice și organizatorice pentru îndeplinirea obligațiilor referitoare la securitatea și controlul sistemelor informatice, în vederea asigurării confidențialității datelor și informațiilor precum și pentru păstrarea în siguranță a acestora, în cadrul activității curente desfasurate in cadrul Spitalului de Psihiatrie Voila.

**3. Principii ale prelucrării datelor cu caracter personal:**

**Legalitatea:** prelucrarea datelor cu caracter personal sunt prelucrate cu buna-credinta si se face in temeiul si in conformitate cu prevederile legale;

**Scopul bine-determinat:** orice prelucrare de date cu caracter personal se face in scopuri bine determinate, explicite si legitime,

adevrate, pertinente si neexcesive prin raportare la scopul in care sunt colectate si ulterior prelucrate;

**Confidentialitatea:** persoanele care prelucreaza, in numele unei institutii, date cu caracter personal au prevazut in contractul de munca si in fisa postului o clauza de confidentialitate;

**Consimtamantul persoanei vizate:** orice prelucrare de date cu caracter personal, cu exceptia prelucrarilor care vizeaza date din categoriile mentionate in Legea nr. 677/2001 si alte date prevazute de acte normative;

**Informarea:** persoana este informata de catre institutia care prelucreaza datele personale ale persoanei vizate – prin consimtamantul informat la momentul internarii sau dreptul la informare afisat in spital;

**Stocarea:** datele cu caracter personal nu se stocheaza pentru o perioada mai lunga decat este necesar pentru realizarea scopurilor in care au fost colectate.

**Protejarea persoanelor vizate:** persoanele vizate au dreptul de acces la datele care sunt prelucrate, de a interveni asupra acestora, de opozitie si de a nu fi supus unei decizii individuale, precum si dreptul de a se adresa Autoritatii Nationale de Supraveghere a Prelucrarii Datelor cu Caracter Personal sau instantei de judecata pentru apararea oricaror drepturi garantate de lege, care le-au fost incalcate;

**Securitatea:** masurile tehnice si organizatorice de securitate a datelor cu caracter personal sunt stabilite astfel incat sa asigure un nivel adecvat de securitate a datelor cu caracter personal procesate, in ceea ce priveste distrugerea accidentala sau ilegala, pierderea, modificarea, dezvaluirea sau accesului neautorizat.

#### **4. Domeniul de aplicare:**

Măsurile tehnice și organizatorice pentru îndeplinirea obligațiilor referitoare la securitatea și controlul sistemelor informatice se impun la nivelul următoarelor compartimente:

- Sectiile si compartimentele medicale.
- Laborator.
- Farmacie.
- Camera de garda.
- Ambulatoriul integrat al spitalului.
- Compartiment statistica si informatica medicala.

## **5. Legislație:**

- Legea nr. 95 din 14 aprilie 2006 privind reforma în domeniul sănătății ( cu modificările și completările ulterioare ).
- ORDIN nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal.
- Legea 677/2001 privind protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, cu modificările și completările ulterioare.

## **6. Definiții:**

- cerințe minime de securitate - complex de măsuri tehnice, informatice, organizatorice, logistice, proceduri și politici de securitate prin care să se asigure nivelul minim de securitate prevăzut în art. 20 din Legea nr. 677/2001.
- utilizator - orice persoană fizică care acționează sub autoritatea operatorului, a persoanei împuternicite sau a reprezentantului, cu drept recunoscut de acces la bazele de date cu caracter personal.

## **7. Descrierea măsurilor organizatorice și tehnice implementate:**

### **a) Identificarea și autentificarea utilizatorului**

Prin utilizator se înțelege orice persoană care acționează sub autoritatea spitalului, a persoanei împuternicite sau a reprezentantului, cu drept recunoscut de acces la bazele de date cu caracter personal.

Utilizatorii, pentru a căpăta acces la o bază de date cu caracter personal, trebuie să se identifice prin introducerea codului de identificare de la tastatură (un șir de caractere). Fiecare utilizator are propriul său cod de identificare. Niciodată nu este alocat același cod de identificare mai multor utilizatori.

Codurile de identificare (sau conturi de utilizator) nefolosite o perioadă mai îndelungată sunt dezactivate și distruse după un control prealabil intern.

Orice cont de utilizator este însoțit de o modalitate de autentificare, respectiv prin introducerea unei parole. Parolele sunt șiruri de caractere, adecvate din punct de vedere al securității ca lungime și compoziție. La introducerea parolilor acestea nu sunt afișate în clar pe monitor. Parolele sunt schimbate periodic în funcție de politicile de

securitate ale spitalului. Schimbarea periodică a parolelor se face numai de către utilizatori autorizați de spital.

Spitalul are implementate un sistem informațional care refuză automat accesul unui utilizator după 5 introduceri greșite ale parolei.

Orice utilizator care primește un cod de identificare și un mijloc de autentificare este obligat prin fișa postului să păstreze confidențialitatea acestora și să răspundă în acest sens în fața operatorului.

Accesul utilizatorilor la bazele de date cu caracter personal efectuate manual se face numai pe baza listei aprobate de conducerea entității – prevazuta în anexa 1.

## **b) Tipul de acces**

Utilizatorii pot să acceseze numai datele cu caracter personal necesare pentru îndeplinirea atribuțiilor lor de serviciu. Pentru aceasta sunt stabilite tipurile de acces după funcționalitate (administrare, introducere, prelucrare, salvare etc.) și după acțiuni aplicate asupra datelor cu caracter personal (scriere, citire, ștergere), precum și procedurile privind aceste tipuri de acces.

Programatorii sistemelor de prelucrare a datelor cu caracter personal nu au acces la datele cu caracter personal. Spitalul permite accesul programatorilor la datele cu caracter personal numai după ce acestea au fost transformate în date anonime.

Compartimentul care asigură suportul tehnic poate avea acces la datele cu caracter personal pentru rezolvarea unor cazuri excepționale.

Spitalul are modalități stricte prin care se vor distruge datele cu caracter personal. Autorizarea pentru această prelucrare de date cu caracter personal este limitată la câțiva utilizatori, prin atribuțiile posturilor.

Alte măsuri specifice implementate de control al accesului sunt:

- în spațiile destinate desfășurării activității spitalului sunt instalate sisteme de alarmă antiefracție și sisteme de supraveghere video;
- monitorizarea și intervenția în caz de alarmă este asigurată de către firma de paza aflată în contract cu spitalul.

### **c) Colectarea datelor**

Spitalul desemnează utilizatori autorizați pentru operațiile de colectare și introducere de date cu caracter personal într-un sistem informațional.

Orice modificare a datelor cu caracter personal se poate face numai de către utilizatori autorizați, sistemul informațional înregistrând cine a făcut modificarea, data și ora modificării.

Colectarea datelor în spitalul nostru se desfășoară în conformitate cu prevederile Ordinului nr. 1.782/2006 privind înregistrarea și raportarea statistică a pacienților care primesc servicii medicale în regim de spitalizare continuă și spitalizare de zi.

Astfel, la nivelul Spitalului de Psihiatrie Voila, colectarea datelor cu caracter personal aparținând pacienților se face prin intermediul următoarelor sisteme informatice:

- DRG national 2008.
- Sistem administrare spital.
- Sistemul gestionare date pacienti.

### **d) Executia copiilor de siguranta**

Spitalul stabilește 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. Utilizatorii care execută aceste copii de siguranță sunt numiți de spital, într-un număr restrâns. Copiile de siguranță se vor stoca în alte camere, în fișete metalice cu sigiliu aplicat.

Se generează zilnic de către sistemul informatic, în mod automat, un back-up pentru o eventuală recuperare a datelor, în cazul distrugerii sau disfuncționalității sistemelor informațice.

### **e) Computerele și terminalele de acces**

Computerele și alte terminale de acces sunt instalate în încăperi care se pot încuia.

Dacă pe ecran apar date cu caracter personal asupra cărora nu se acționează o perioadă dată, stabilită de spital, sesiunea de lucru se închide automat. Mărimea acestei perioade se determină în funcție de operațiile care trebuie executate.

Serverele care găzduiesc bazele de date ce conțin pacienții pot fi accesate doar în mod controlat, pe baza de drepturi de acces.



## **f) Fișierele de acces**

Spitalul a luat măsuri ca orice accesare a bazei de date cu caracter personal să fie înregistrată într-un fișier de acces (numit log la prelucrările automate).

Informațiile înregistrate în fișierul de acces sunt:

- 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, lună, 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.

Fișierele de acces trebuie să facă posibilă identificarea de către operator sau de către persoana împuternicită a persoanelor care au accesat date cu caracter personal fără un motiv anume, în vederea aplicării unor sancțiuni sau a sesizării organelor competente.

## **g) Sistemele de telecomunicatii**

Spitalul execută periodic controlul autentificărilor și tipurilor de acces pentru detectarea unor disfuncționalități în ceea ce privește folosirea sistemelor de telecomunicații.

Pentru transmisia datelor cu caracter personal se impune folosirea metodei de criptare.

## **h) Instruirea personalului**

În cadrul cursurilor de pregătire a utilizatorilor spitalul face informarea acestora cu privire la:

- prevederile Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date,
- cerințele minime de securitate a prelucrărilor de date cu caracter personal, precum și cu privire la riscurile pe care le comportă

prelucrarea datelor cu caracter personal, în funcție de specificul activității.

- obligativitatea pastrării confidențialității datelor cu caracter personal. Salariaților care au acces la datele cu caracter personal ale pacienților le este interzis să le transfere sau să le utilizeze în alte scopuri decât cele strict profesionale. În acest scop, aceștia sunt obligați să semneze un angajament scris.

Scoaterea la imprimantă a datelor cu caracter personal se va realiza numai de utilizatori autorizați pentru această operațiune de către spital.

#### **i) Folosirea computerelor**

Pentru menținerea securității prelucrării datelor cu caracter personal (în special împotriva virușilor informațici) spitalul va lua măsuri care vor consta în:

- interzicerea folosirii de către utilizatori a programelor software care provin din surse externe sau dubioase;
- informarea utilizatorilor în privința pericolului privind virușii informațici;
- implementarea unor sisteme automate de devirusare și de securitate a sistemelor informatice;

Intocmit: **As. Social Boeru Daniela**

Verificat: **Jr. Lupu Livia**

Avizat: **Ec. Felea Monica – Director Financiar Contabil**