SPITALUL DE PSIHIATRIE VOILA
Mun. Campina, str. Voila nr. 114, jud. Prahova
TEL: 0244 / 335 161; FAX: 0344-102034
E-mail: spitalpsihiatrie@clicknet.ro; Web: 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), veti lua la cunostinta asupra "Notei de informare privind protectia datelor personale".

2. **Scopul documentului:** prezentul document reglementeaza măsurile tehnice şi organizatorice pentru îndeplinirea obligaţiilor referitoare la securitatea şi controlul sistemelor informatice, în vederea asigurării confidenţialităţii datelor şi informaţiilor precum şi pentru păstrarea în siguranţă a acestora, în cadrul activităţii curente desfasurate in cadrul Spitalului de Psihiatrie Voila.

## 3. Principii ale prelucrarii 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,

adecvate, 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 în 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 în 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 încat sa asigure un nivel adecvat de securitate a datelor cu caracter personal procesate, în ceea ce priveste distrugerea accidentala sau ilegala, pierderea, modificarea, dezvaluirea sau accesului neautorizat.

## 4. Domeniul de aplicare:

Măsurile tehnice şi organizatorice pentru îndeplinirea obligaţiilor referitoare la securitatea şi controlul sistemelor informatice se impun la nivelul urmatoarelor compartimente:

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

5. **Legislaţie:**

- Legea nr. 95 din 14 aprilie 2006 privind reforma în domeniul sănătăţii ( cu modificările şi completările ulterioare ).
- ORDIN nr. 52 din 18 aprilie 2002 privind aprobarea Cerinţelor minime de securitate a prelucrărilor de date cu caracter personal.
- Legea 677/2001 privind protectia persoanelor cu privire la prelucrarea datelor cu character personal si libera circulatie a acestor date, cu modificarile si completarile ulterioare.

6. **Definitii:**

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

7. **Descrierea masurilor organizatorice şi tehnice implementate:**

**a) Identificarea si autentificarea utilizatorului**

Prin utilizator se înţelege orice persoană care acţionează 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 şir de caractere). Fiecare utilizator are propriul său cod de identificare. Niciodată nu este alocat acelaşi cod de indentificare mai multor utilizatori.

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

Orice cont de utilizator este însoţit de o modalitate de autentificare, respectiv prin introducerea unei parole. Parolele sunt şiruri de caractere, adecvate din punct de vedere al securităţii ca lungime şi compoziţie. La introducerea parolelor acestea nu sunt afişate în clar pe monitor. Parolele sunt schimbate periodic în funcţie de politicile de

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

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

Orice utilizator care primeşte un cod de identificare şi un mijloc de autentificare este obligat prin fişa postului să păstreze confidenţialitatea acestora şi să răspundă în acest sens în faţa operatorului.

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

**b) Tipul de acces**

Utilizatorii pot să accesa numai datele cu caracter personal necesare pentru îndeplinirea atribuţiilor lor de serviciu. Pentru aceasta sunt stabilite tipurile de acces după funcţionalitate (administrare, introducere, prelucrare, salvare etc.) şi după acţiuni aplicate asupra datelor cu caracter personal (scriere, citire, ştergere), precum şi 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 excepţionale.

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

Alte măsuri specifice implementate de control al acesulului sunt:

- în spaţiile destinate desfăşurării activităţii spitalului sunt instalate sisteme de alarmă antiefracţie si sisteme de supraveghere video;
- monitorizarea şi intervenţia în caz de alarmă este asigurată de catre firma de paza aflata in contract cu spitalul.

**c) Colectarea datelor**

Spitalul desemnează utilizatori autorizaţi pentru operaţiile de colectare şi introducere de date cu caracter personal într-un sistem informaţional.

Orice modificare a datelor cu caracter personal se poate face numai de către utilizatori autorizaţi, sistemul informaţional înregistrand cine a făcut modificarea, data şi ora modificării.

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

Astfel, la nivelul Psitalului de Psihiatrie Voila, colectarea datelor cu caracter personal apartinand pacientilor se face prin intermediul urmatoarelor sisteme informatice:

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

**d) Executia copiilor de siguranta**

Spitalul stabileşte intervalul de timp la care se vor executa copiile de siguranţă ale bazelor de date cu caracter personal, precum şi ale programelor folosite pentru prelucrările automatizate. Utilizatorii care execută aceste copii de siguranţă sunt numiţi de spital, într-un număr restrâns. Copiile de siguranţă se vor stoca în alte camere, în fişete 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 disfuncţionalităţii sistemelor informaţice.

**e) Computerele si terminalele de acces**

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

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

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

## f) Fisierele de acces

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

Informaţiile înregistrate în fişierul de acces sunt:

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

Pentru prelucrările automate aceste informaţii vor fi stocate într-un fişier de acces general sau în fişiere separate pentru fiecare utilizator. Orice încercare de acces neautorizat va fi, de asemenea, înregistrată.

Fişierele 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 sancţiuni sau a sesizării organelor competente.

## g) Sistemele de telecomunicatii

Spitalul execută periodic controlul autentificărilor şi tipurilor de acces pentru detectarea unor disfuncţionalităţi în ceea ce priveşte folosirea sistemelor de telecomunicaţii.

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 protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date,
- cerinţele minime de securitate a prelucrărilor de date cu caracter personal, precum şi cu privire la riscurile pe care le comportă

prelucrarea datelor cu caracter personal, în funcţie de specificul activităţii.

- obligativitatea pastrarii confidenţialitatii datelor cu caracter personal.

Salariatilor care au acces la datele cu caracter personal ale pacientilor le este interzis să le transfere sau să le utilizeze în alte scopuri decât cele strict profesionale. În acest scop, aceştia sunt obligaţi să semneze un angajament scris.

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

**i) Folosirea computerelor**

Pentru menţinerea securităţii prelucrării datelor cu caracter personal (în special împotriva viruşilor informaţici) 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 privinţa pericolului privind viruşii informatici;
- implementarea unor sisteme automate de devirusare şi de securitate a sistemelor informatice;

**Intocmit: As. Social Boeru Daniela**

**Verificat: Jr. Lupu Livia**

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