

CONSILIUL JUDEȚEAN BRAȘOV
SPITALUL CLINIC DE PSIHIATRIE ȘI NEUROLOGIE BRAȘOV
STR. PRUNDULUI nr. 7-9 BRAȘOV
Tel. 0268/511481 Fax. 0268/410205
Nr. 12389 / 13.08.2018

Operator de date cu caracter personal nr. 9275



REGULAMENT INTERN AL SPITALULUI CLINIC DE PSIHIATRIE ȘI NEUROLOGIE BRAȘOV ÎN CONFORMITATE CU REGULAMENTUL NR. 679/27.04.2016 PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL

OBIECT-OBIECTIV

Prezentul regulament stabilește normele referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, precum și normele referitoare la libera circulație a datelor cu caracter personal.

DOMENIUL DE APLICARE

Prezentul regulament se aplică prelucrării datelor cu caracter personal, efectuată total sau parțial prin mijloace automatizate precum și prelucrării prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidență a datelor.

SPITALUL CLINIC DE PSIHIATRIE ȘI NEUROLOGIE BRAȘOV înscris în registrul de **evidență a prelucrării de date cu caracter personal nr. 9275**, prin intermediul Biroului de Informatică și Statistică Medicală prelucrează datele pacienților cu caracter personal: codul numeric personal, seria și numărul actului de identitate, date privind starea de sănătate s.a., prin mijloace automatizate /manual având ca scop "servicii de sănătate".

Totodată SCPN prelucrează datele cu caracter personal ivite în legătură cu apariția raporturilor de muncă /serviciu ale angajaților, prin Serviciul RUNOS.

DEFINITII

Date cu caracter personal- inseamna orice informatii privind o persoana fizica identificata sau identificabila (o persoana vizata); o persoana identificabila este o persoana care poate fi identificata, direct sau indirect, in special prin referire la un element de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identitatii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;

Prelucrare- inseamna orice operatiune sau set de operatiuni efectuate asupra datelor cu caracter personal sau asupra datelor cu caracter personal, cu sau fara utilizarea de mijloace automatizate;

Date privind sanatatea- inseamna date cu caracter personal legate de sanatatea fizica sau mintala a unei persoane fizice, inclusiv prestarea de servicii de asistenta medicala, care dezvaluie informatii despre starea de sanatate a acesteia;

Stocarea- păstrarea pe orice fel de suport a datelor cu caracter personal culese;

Sistem de evidență a datelor cu caracter personal– orice structură organizată de date cu caracter personal, accesibilă potrivit unor criterii determinate, indiferent dacă această structură este organizată în mod centralizat ori descentralizat sau este repartizată după criteriile funcționale ori geografice;

Operator – orice persoană fizică sau juridică, de drept privat ori de drept public, inclusiv autoritățile publice, instituțiile și structurile teritoriale ale acestora, care stabilește scopul și mijloacele de prelucrare a datelor cu caracter personal; dacă scopul și mijloacele de prelucrare a datelor cu caracter personal sunt determinate printr-un act normativ sau în baza unui act normativ, operator este persoana fizică sau juridică, de drept public ori de drept privat, care este desemnată ca operator prin acel act normativ sau în baza acelui act normativ;

Persoană împuternicită de către operator – o persoană fizică sau juridică, de drept privat ori de drept public, inclusiv autoritățile publice, instituțiile și structurile teritoriale ale acestora, care prelucrează date cu caracter personal pe seama operatorului;

Terț – orice persoană fizică sau juridică, de drept privat ori de drept public, inclusiv autoritățile publice, instituțiile și structurile teritoriale ale acestora, alta decât persoana vizată, operatorul ori persoana împuternicită sau persoanele care, sub autoritatea directă a operatorului sau a persoanei împuternicite, sunt autorizate să prelucreze date;

Destinatar – orice persoană fizică sau juridică, de drept privat ori de drept public, inclusiv autoritățile publice, instituțiile și structurile teritoriale ale acestora, căreia îi sunt dezvăluite date, indiferent dacă este sau nu terț; autoritățile publice cărora li se comunică date în cadrul unei competențe speciale de anchetă nu vor fi considerate destinatari;

Date anonime – date care, datorită originii sau modalității specifice de prelucrare, nu pot fi asociate cu o persoană identificată sau identificabilă;

Consimțământ – orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;

Persoana vizată – persoana fizică ale cărei date cu caracter personal sunt prelucrate în următoarele scopuri:

- 1) personalul angajat, delegat și detașat
- 2) persoana care este parte sau face demersuri înainte de încheierea unui contract cu operatorul;
- 3) persoana care aplică pentru posturile/locurile de munca scoase la concurs de operator;

A dezvălui – a transmite, a distribui, a face disponibile în orice alt mod date cu caracter personal, în afara operatorului;

A utiliza – a se folosi datele cu caracter personal de către și în interiorul operatorului;

Caracteristicile datelor cu caracter personal în cadrul prelucrării

Datele cu caracter personal destinate a face obiectul prelucrării trebuie să fie:

- a) prelucrate cu bună-credință și în conformitate cu dispozițiile legale în vigoare;
- b) colectate în scopuri determinate, explicite și legitime. Prelucrarea ulterioară a datelor cu caracter personal în scopuri statistice, nu va fi considerată incompatibilă cu scopul colectării dacă se efectuează cu respectarea dispozițiilor legii, inclusiv a celor care privesc efectuarea notificării către autoritatea de supraveghere, precum și cu respectarea garanțiilor privind prelucrarea datelor cu caracter personal, prevăzute de normele care reglementează activitatea statistică;
- c) adecvate, pertinente și neexcesive prin raportare la scopul în care sunt colectate și ulterior prelucrate;

d) exacte și, dacă este cazul, actualizate, în acest scop se vor lua măsurile necesare pentru ca datele inexacte sau incomplete din punct de vedere al scopului pentru care sunt colectate și pentru care vor fi ulterior prelucrate, să fie șterse sau rectificate;

e) stocate într-o formă care să permită identificarea persoanelor vizate strict pe durata necesară realizării scopurilor în care datele sunt colectate și în care vor fi ulterior prelucrate. Stocarea datelor pe o durată mai mare decât cea menționată, în scopuri statistice, se va face cu respectarea garanțiilor privind prelucrarea datelor cu caracter personal, prevăzute în normele care reglementează acest domeniu, și numai pentru perioada necesară realizării acestor scopuri.

ORGANIZAREA MASURILOR DE PROTECTIE A DATELOR MEDICALE CU CARACTER PERSONAL

Documentatia medicala, inclusiv fisele medicale ale pacientilor inregistrati in cadrul spitalului, inclusiv alte formulare si registre care contin date cu caracter personal si medical se considera purtatoare de **date cu caracter personal**.

Aceasta documentatie urmeaza a fi pastrata de catre angajatii institutiei in birouri si spatii special destinate (arhiva, statistica, birouri medici si asistente medicale, laboratoare)

Dupa externarea pacientilor, foile de observatie sunt pastrate in arhiva spitalului in conformitate cu cerintele nomenclatorului arhivistic/legislatia in vigoare

Transmiterea fiselor medicale catre alte sectii se asigura numai prin personalul medical si auxiliar sanitar responsabil

Nu se permite eliberarea foilor de observatie, in original, pacientilor (reprezentantilor acestora s.a)

In scopul evitarii divulgarii datelor cu caracter personal si medical se cere obligatoriu stabilirea identitatii persoanei care receptioneaza fisele medicale prin verificarea actului de identitate /legitimatiei de serviciu /etc

Nu se permit discutii prin telefon referitor la datele cu caracter personal si medical

CONSIMITAMANTUL LA PRELUCRAREA DATELOR CU CARACTER PERSONAL SI MEDICAL

Datele personale ale pacientilor sunt prelucrate (preluate, prelucrate, stocate) de catre SCPN, in conformitate cu prevederile Regulamentului UE 679/2016 si

actele normative in vigoare din domeniul sanatatii, in scopul efectuarii de servicii medicale.

***PASTRAREA MASURILOR DE SECURITATE A DATELOR CU
CARACTER PERSONAL SI MEDICAL DE CATRE ANGAJATII SCPN***

- Sefii de sectie/compartimente organizeaza masuri de instruire a persoanelor din subordine privind protectia datelor cu caracter personal avand ca referinta prevederile prezentului Regulament
- Toti salariatii SCPN efectueaza prelucrarea datelor cu caracter personal conform atributiilor functiei
- Nu se admite prelucrarea datelor cu caracter personal in alte scopuri decat in scopul exercitarii obligatiilor legale
- Nu se admite divulgarea datelor medicale cu caracter personal, persoanelor terte prin telefon sau prin comunicare directa fara stabilirea identitatii persoanei si a termenului legal al solicitarii
- Nu se admite divulgarea datelor medicale cu caracter personal in discutii intre salariatii, cu exceptia cazurilor de necesitate de serviciu
- Personalul medical este obligat sa explice pacientilor, solicitantilor motivele nedivulgarii datelor medicale cu caracter personal, sau refuzul eliberarii unor documente medicale, etc.
- Computerele, serverele, alte terminale de acces sunt amplasate in locuri cu acces limitat pentru persoane straine
- Sefii de servicii, personalul medical trebuie sa organizeze la locul de munca plasarea obiectivelor ce contin date cu caracter personal in asa fel incat sa raspunda necesitatii asigurarii securitatii acestora contra accesului nepermis, furturilor, incendiilor, inundatiilor si altor posibile riscuri.

***SECURITATEA DATELOR CU CARACTER PERSONAL/MEDICAL ,
PRELUCRAREA ACESTORA IN MOD MANUAL(PE SUPORT DE
HARTIE) IN CADRUL SCPN***

- Fisele medicale din cadrul spitalului (FOCG, formulare, registre) se considera purtatoare de date cu caracter personal

- Foile de observatie clinica generala ale tuturor pacientilor inregistrati in cadrul SCPN sunt pastrate pana la arhivare in cadrul Biroului de Informatica si Statistica Medicala
- Nu sunt permise discutii la telefon referitoare la date cu caracter personal
- Acordarea asistentei medicale prevede prelucrarea datelor cu caracter personal
- Datele cu caracter personal ale beneficiarilor de servicii prestate de catre SCPN sunt prelucrate in scopul efectuarii de servicii medicale.
- Refuzul pacientului privind furnizarea datelor cu caracter personal nu va afecta calitatea ingrijirilor si tratamentul de care beneficiaza in cadrul SCPN, **in situatia** in care prelucrarea este necesara pentru prevenirea unui pericol iminent.
- Informatiile inregistrate cu privire la datele cu caracter personal ale pacientilor sunt destinate utilizarii de catre operator si sunt comunicate urmatoarelor destinatari:
 - Casa de Asigurări de Sănătate – C.A.S., Direcția de Sănătate Publică – D.S.P., Dosarul Electronic de Sănătate – D.E.S., Școala Națională de Sănătate Publică, Management și Perfecționare în Domeniul Sanitar București - S.N.S.P.M.P.D.S.B., Autoritatea Naționala de Management al Calității în Sănătate – A.N.M.C.S., Inspectoratul Teritorial de Muncă – diverse societati care au ca obiect prestare de servicii medicale și care au încheiate contracte de prestări servicii cu unitatea noastră (ex. efectuare de investigații de imagistică medicală- RMN, CT, investigații de laborator prin prelevare de produse biologice), consulturi interdisciplinare efectuate în alte unități medicale, etc.
 - Organe competente (instante judecatoresti), organe de cercetare (Parchet, Politie)

SISTEMUL INFORMATIONAL DE PRELUCRARE A DATELOR CU CARACTER PERSONAL DIN CADRUL SCPN

Datele cu caracter personal care se prelucreaza sunt urmatoarele:

- Nume, Prenume
- Data si locul nasterii
- CNP
- Sexul

- Adresa, domiciliu, resedinta
- Date privind sanatatea
 - Sistemul informational de prelucrare a datelor cu caracter personal din cadrul spitalului este alcatuit din urmatoarele elemente (mijloace tehnice si soft)
- Statie de lucru
- Servere
 - Toti utilizatorii (inclusiv personalul care asigura sustinerea tehnica, administratorul de retea, programatori, administratori ai bazelor de date) au un indentificator personal(ID-ul utilizatorului). Pentru confirmarea ID-ului utilizatorului sunt utilizate parole irepetabile de nu mai putin de 7-8 caractere ce contin litere din ambele registre, cifre si alte semne simbolice.

Administrarea identificatorilor utilizatorilor include:

- identificarea univoca (irepetitiva) al fiecarui utilizator
- verificarea autenticitatii fiecarui utilizator
- garantarea factorului ca ID-ul utilizatorului este eliberat unei persoane determinate complet
- dezactivarea contului de utilizator dupa o perioada inactiva stabilita in timp

Reguli de asigurare a securitatii informationale

Regulile de asigurare a securitatii informationale in cazul alegerii si folosirii parolei include:

- Pastrarea confidentialitatii parolelor
- Interzicerea inscrierii parolelor pe suport de hartie, in cazul in care nu se asigura securitatea pastrarii acestora
- Modificarea parolelor de fiecare data cand sunt prezente indiciile eventualei compromiteri a sistemului sau a parolei
- Alegerea parolelor calitative cu o marime de minim 7-8 simboluri , care nu contin simboluri identice consecutive si nu sunt compuse integral din grupul de cifre sau litere
- Este asigurata posibilitatea utilizatorilor de a alege si schimba parolele individuale
- Este asigurata blocarea accesului dupa 5 tentative gresite de autentificare
- Inainte de acordarea accesului in sistem, utilizatorii sunt informati despre faptul ca folosirea sistemelor informationale de date cu caracter personal este

controlata si ca utilizarea neautorizata a acestora se urmareste in conformitate cu legislatia

- Totodata se asigura protectia contra infiltrarii programelor daunatoare in softuri destinate prelucrarii datelor cu caracter personal, masura ce asigura posibilitatea reinnoirii automate si la timp a mijloacelor de asigurare a protectiei contra programelor daunatoare si a virusilor
- Controalele de securitate a informatiilor de date cu caracter personal se efectueaza cu regularitate cel putin o data pe an .

REGULI CU PRIVIRE LA PROTECTIA DATELOR CU CARACTER PERSONAL IN CADRUL SERVICIULUI R.U.N.O.S.

- Aceste reguli se refera la stabilirea masurilor telefonice si organizatorice necesare pentru asigurarea sanatatii, a confidentialitatii si integritatii datelor cu caracter personal in cadrul Serviciului RUNOS. Orice informatie referitoare la angajati, reflectata in sistemul informational, in dosarul personal, fisa personala, contractul individual de munca, acte aditionale la CIM, diverse registre specifice Serviciului RUNOS sunt considerate date cu caracter personal
- Colectarea si prelucrarea datelor personale ale salariatului poate fi efectuata exclusiv in scopul angajarii, instruirii, avansarii in serviciu, atestarii, perfectionarii, furnizarii datelor catre: Colegiul Medicilor, Ordinul Asistentilor, I.T.M., Casa de Pensii, Directia de Sanatate si Asistenta Medicala Brasov, Consiliul Judetan Brasov, Ministerul Sanatatii, Directia de Sanatate Publica, Medicina Muncii, Casa de Asigurari, A.N.A.F., etc;
- Serviciul RUNOS este obligat sa utilizeze datele cu caracter personal ale salariatilor numai in limitele competentelor functionale, doar in timpul orelor de program.
- Serviciul RUNOS are obligatia sa excluda sau sa rectifice la solicitarea salariatului datele personale incorecte sau incomplete si a informatiilor care se pastreaza nelegitim
- Serviciul RUNOS nu are dreptul sa obtina si sa prelucreze date referitoare la convingerile politice, religioase, la viata privata.

- Serviciul RUNOS nu are dreptul sa obtina si sa prelucreze date privind apartenenta salariatului la sindicate, asociatii religioase, partide si alte organizatii social politice
- Serviciul RUNOS nu trebuie sa comunice unor terti datele personale ale salariatilor fara acordul scris al acestuia cu exceptia cazurilor prevazute de lege si respectand ierarhizarea de subordonare a Spitalului (M.S, D.S.P.,D.S.A.M., C.J. Bv , C.A.S Bv, Finante, Pensii , I.T.M., Ordinul Asistentilor, Colegiul Medicilor etc)
- Serviciul RUNOS trebuie/poate sa permita accesul la datele personale ale salariatului doar persoanelor imputernicite necesare exercitarii unor atributii de serviciu (manager, director medical, director financiar contabil, sindicat si altora in conformitate cu legislatia in vigoare)
- Serviciul RUNOS are obligatia sa previna persoanele, care in exercitiul functiunii solicita si primesc date cu caracter personal ale salariatilor ca poarta raspundere, in conformitate cu legislatia in vigoare pentru divulgarea lor, luandu-se in considerare prejudiciul adus prin acestea salariatului .
- De comun acord cu Biroul de Informatica si Statistica Medicala, Serviciul RUNOS, trebuie sa asigure protectia datelor cu caracter personal in procesul exploatarei sistemului informational, prevenirea scurgerii informatiei, distrugerii, modificarii, copierii.
- Nu se admite in cadrul Serviciului RUNOS accesul neautorizat la datele cu caracter personal ale salariatilor sau accesul neautorizat al persoanelor straine
- Predarea datelor cu caracter personal de catre Serviciul RUNOS in arhiva institutiei se face conform nomenclatorului arhivistic aprobat.

SECURITATEA SERVICIULUI R.U.N.O.S.:

- Dulapurile cu dosarele salariatilor sunt permanent inchise
- La sfarsitul programului de munca se incuie usile si ferestrele
- Nu se admite accesul persoanelor straine la computer
- Respectarea cerintelor si asigurarea securitatii contra incendiilor si altor posibile riscuri

In ceea ce priveste asigurarea protectiei datelor personale care se pastreaza in cadrul Serviciului RUNOS, salariatul are dreptul:

- De a primi informatia deplina despre datele sale personale si modul de prelucrare ale acestora

- De a avea acces liber si gratuit la datele sale personale, inclusiv dreptul la o copie de pe orice act juridic care contine datele personale
- De a cere excluderea sau rectificarea datelor personale incorecte sau incomplete, a informatiilor care se pastreaza nelegitim
- De a ataca in instanta de judecata orice actiune sau inactiune ilegala a angajatorului referitoare la obtinerea, pastrarea, prelucrarea si protectia datelor personale ale salariatului.
- Personalul Serviciului RUNOS si alte persoane care, in exercitiul functiunii au luat cunostinta de datele cu caracter personal, raspund in conformitate cu legislatia in vigoare pentru divulgarea acestor date, luandu-se in considerare prejudiciul adus de catre acestea.

***REGULAMENTUL PRIVIND ASIGURAREA SECURITATII DATELOR
CU CARACTER PERSONAL AL PACIENTULUI IN CADRUL SCPN***

Regulamentul are ca scop asigurarea nivelului corespunzator al protectiei datelor cu caracter personal tuturor persoanelor care beneficiaza de servicii medicale prin aplicarea corespunzatoare a legislatiei in vigoare cu privire la protectia datelor.

Scopul prelucrării datelor cu caracter personal in cadrul spitalului este prestarea serviciilor medicale acordate pacientilor. Toate fisele medicale ale pacientilor din ambulatoriu, camera de garda, foile de observatie ale pacientilor internati in sectiile spitalului, inclusiv alte formulare si registre, fise pe suport de hartie, note la cazurile de deces, certificate extrase, trimiteri la investigatii, care contin date cu caracter personal, se considera purtatoare de date cu caracter personal.

Pentru realizarea scopului de prestare a serviciilor medicale, medicii si asistentii medicali sunt in drept de a solicita de la persoana care se adreseaza pentru acordarea asistentei medicale in unitate, urmatoarele date:

- Numele, prenumele
- Data si locul nasterii
- CNP
- Cardul de sanatate
- Numarul de telefon
- Adresa de domiciliu
- Profesia si/sau locul de munca
- Semnatura
- Cetatenia

In vederea respectarii confidentialitatii datelor cu caracter personal, personalul medical va respecta cu strictete urmatoarele reguli:

- Toate documentele medicale ce contin date cu caracter medical si personal urmeaza a fi pastrate in locuri special destinate in dulapuri care se incuie
 - Nu se admite divulgarea datelor cu caracter personal in discutii intre salariati, cu exceptia cazurilor care prezinta interes de serviciu
 - Acordarea asistentei medicale este initiata la etapa de programare a pacientului si prevede prelucrarea datelor cu caracter personal
 - Datele cu caracter personal ale persoanelor care beneficiaza de servicii medicale in cadrul SCPN sunt prelucrate (preluate, prelucrate, stocate), in conformitate cu prevederile Regulamentului UE 679/2016 si actele normative in vigoare din domeniul sanatatii, in scopul efectuarii de servicii medicale.
- In conformitate cu Regulamentul UE nr.679/2016, persoana vizata isi poate exercita drepturile de acces, de interventie si de opozitie.

***REGULAMENT PRIVIND SUPRAVEGHEREA
PRIN MIJLOACE VIDEO IN CADRUL SPITALULUI CLINIC DE
PSIHIATRIE ŞI NEUROLOGIE BRASOV***

În contextul actual securitatea obiectivelor nu poate fi asigurată fără o supraveghere video eficientă, care să permită atat monitorizarea în timp real a evenimentelor și persoanelor suspecte, cat și înregistrarea imaginilor video.

Totodată, utilizarea unui astfel de sistem include anumite responsabilități și garanții din partea proprietarului de sistem, referitor la prelucrarea și protecția datelor cu caracter personal care se înregistrează în sistem.

Din acest motiv, este necesară stabilirea unui regulament de securitate privind supravegherea prin mijloace video și prelucrarea datelor cu caracter personal preluate și înregistrate în sistemul de monitorizare prin înregistrare video.

Regulamentul privind supravegherea prin mijloace video în cadrul SCPN are ca scop:

- Stabilirea unui set unitar de reguli care reglementează implementarea și utilizarea sistemului de supraveghere video, în scopul asigurării securității persoanelor și bunurilor, pazei și protecției bunurilor, imobilelor, valorilor și a materialelor cu regim special, respectând în același timp obligațiile ce revin entității, în calitate de operator de date, conform legislației in vigoare (Legea nr.333/2003) și măsurile de securitate adoptate pentru protecția datelor cu

caracter personal, protejarea vieții private, a intereselor legitime și garantarea drepturilor fundamentale ale persoanelor vizate.

- Stabilirea responsabilităților privind administrarea și exploatarea sistemului de supraveghere prin mijloace video, precum și cele privind întocmirea, avizarea și aprobarea documentelor aferente acestor activități.

- Scopul utilizării sistemului video este de a asigura buna administrare și funcționare a entității, în special în vederea controlului de securitate și pază. De asemenea, sistemul video este necesar pentru a sprijini politicile de securitate instituite de actele normative care reglementează protecția datelor cu caracter personal și contribuie la îndeplinirea atribuțiilor structurii de securitate.

- Prezentul Regulamentul descrie măsurile care necesită a fi luate de către spital pentru a proteja datele cu caracter personal care sunt prelucrate prin metoda supravegherii video, vieții private și alte drepturi fundamentale și interese legitime ale subiecților.

Zonele supravegheate

Camerele de supraveghere video sunt amplasate în locuri vizibile. Orice utilizare ascunsă a acestora este strict interzisă, cu excepția cazurilor expres reglementate de legislație.

Nu sunt monitorizate zonele în care persoanele pot conta, în mod rezonabil, pe intimitate, precum birourile de serviciu și toaletele.

Datele cu caracter personal colectate prin intermediul sistemului de supraveghere video

Sistemul de supraveghere video este dotat cu detector de mișcare. Toate camerele funcționează în regim 24/24 ore și sunt fixate. La darea în exploatare a sistemului de supraveghere video, persoana împuternicită va primi instructajul referitor la setările sistemului de monitorizare video, respectarea regimului de confidențialitate și dreptul de acces la informația prelucrată în sistemul de evidență.

Limitarea scopului

Sistemul de supraveghere video va fi utilizat numai în scopul în care este notificat, fără a se urmări în special obținerea unor informații pentru anchetele interne sau procedurile disciplinare, cu excepția situațiilor în care se produce un incident de securitate sau se observă un comportament infracțional (în circumstanțe excepționale imaginile pot fi transmise organelor competente în cadrul unor investigații disciplinare sau penale).

Persoana responsabilă va gestiona accesul la sistemul de supraveghere video numai cu acordul scris al conducerii spitalului.

Categoriile speciale de date cu caracter personal

Sistemul de monitorizare video al SCPN nu are ca scop captarea (spre exemplu prin focalizare sau orientare selectivă) sau prelucrarea imaginilor (spre exemplu indexare, creare de profiluri) care constituie categoria specială de date cu caracter personal.

Accesul la datele cu caracter personal și dezvoltarea acestora

Accesul la imaginile video înregistrate în timp real este limitat la un număr redus de angajați ai spitalului care pot fi identificați individual, în conformitate cu lista aprobată de către conducerea unității.

Accesul la imaginile video și/sau la arhiva în care sînt stocate imaginile înregistrate este permis numai persoanei responsabile din cadrul spitalului.

Drepturi de acces

1. Accesul la imaginile stocate și/sau la arhitectura tehnică a sistemului de supraveghere video este limitat la un număr redus de persoane și este determinat prin atribuțiile specificate în fișa postului, în care este indicat în ce scop și ce tip de acces este acordat.

2. SCPN impune limite stricte în privința persoanelor care au dreptul:

- să vizioneze materialul filmat în timp real: imaginile care se derulează în timp real sunt accesibile responsabililor de securitate și agenților de pază desemnați să desfășoare activitatea de supraveghere;

- să vizioneze înregistrarea materialului filmat: vizionarea imaginilor înregistrate se va face în cazuri justificate, cum ar fi cazurile prevăzute expres de lege și incidentele de securitate, de către persoanele special desemnate;

- să copieze, să descarce, să șteargă sau să modifice orice material filmat de sistemul de supraveghere video.

3. Instrucțaj

Toți membrii personalului cu drepturi de acces beneficiază de o instruire inițială în domeniul protecției datelor.

Această procedură va fi integrată în programul de instruire și îndrumare, pentru toți utilizatorii cu drept de acces și atribuții în operarea sistemului de supraveghere video.

4. Măsuri de păstrare a confidențialității

Dezvăluirea datelor cu caracter personal

Orice activitate de dezvăluire a datelor personale către terți va fi documentată și supusă unei analize riguroase privind pe de-o parte necesitatea comunicării, și pe de altă parte compatibilitatea dintre scopul în care se face comunicarea și scopul în care aceste date au fost colectate inițial pentru prelucrare.

Orice situație de dezvăluire va fi consemnată de administratorul sistemului într-un Registru de evidență special.

Spitalul are obligația punerii la dispoziția organelor judiciare, la solicitarea formulată în scris a acestora, înregistrările video în care este surprinsă săvârșirea unor fapte de natură contravențională/penală.

Sistemul de supraveghere video nu este utilizat pentru evaluarea performanței la locul de muncă.

Durata păstrării înregistrărilor video

Durata păstrării înregistrărilor video este de 30 zile calendaristice, după care acestea se sterg automat în ordinea în care au fost înregistrate.

În cazul producerii unui incident de securitate, durata de păstrare a înregistrărilor video poate depăși limitele admisibile de program, în funcție de timpul necesar investigației suplimentare a incidentului de securitate.

Informarea publicului referitor la supravegherea video

Informarea publicului referitor la supravegherea video din cadrul SCPN se efectuează prin pictograme.

SCPN garantează că asigură respectarea drepturilor ce revin persoanelor vizate, în conformitate cu legislația în vigoare. Toate persoanele implicate în activitatea de supraveghere video și cele responsabile de administrarea imaginilor filmate vor respecta procedurile și regulamentele de acces la date cu caracter personal ale entității.

Informarea persoanelor vizate

Informarea primară a persoanelor vizate se realizează în mod clar și permanent, prin intermediul unui semn adecvat, cu vizibilitate suficientă și localizat în zona supravegheată, astfel încât să semnaleze existența camerelor de supraveghere, dar și pentru a comunica informațiile esențiale privind prelucrarea datelor cu caracter personal.

Persoanele vizate sunt atenționate asupra existenței sistemului de supraveghere video prin note de informare corespunzătoare.

Întocmit,
Responsabil cu protecția datelor
Jr. Simona Gârea