

DECIZIE

Nr.: 243/14.06.2022

Managerul Institutului Oncologic "Prof. Dr. Ion Chiricuță", Cluj-Napoca (I.O.C.N.), Șef
Lucr. Dr. Vlad Ioan-Cătălin, numit în baza Ordinului Ministrului Sănătății nr. 1394/ 29.07.2021,

În temeiul prevederilor:

- Legii nr. 95/2006 privind reforma în domeniul sănătății republicată, cu modificările și completările ulterioare;
- Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE;
- Legii nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor)
- Orientărilor privind transparența în temeiul Regulamentului (UE) 679/2018
- Avizului nr. 2/2017 privind prelucrarea datelor la locul de muncă
- Ghidul nr. 3/2019 privind prelucrarea datelor cu caracter personal prin mijloace de supraveghere video

DECIDE

Art. 1. – Începând cu data prezentei, se instituie **Politica privind supravegherea video** în cadrul Institutului Oncologic "Prof. Dr. Ion Chiricuță", Cluj-Napoca, având următoarele prevederi:

POLITICA PRIVIND SUPRAVEGHEREA VIDEO

Prezenta Politică se aplică prelucrării datelor cu caracter personal prin mijloace de supraveghere video, având scopul de a oferi informații cu privire la modalitatea în care sunt prelucrate



datele (imaginea) persoanelor care pătrund în raza de acțiune a sistemului de supraveghere video instalat la sediul principal al operatorului de date cu caracter personal.

Politica privind supravegherea video se aplică de către conducerea operatorului și de către personalul desemnat cu administrarea și mentenanța sistemului de supraveghere video.

Art. 1 Operatorul de date cu caracter personal

Institutul Oncologic "Prof. Dr. Ion Chiricuță", Cluj-Napoca, este unitate sanitară cu personalitate juridică ce prelucrează date cu caracter personal, având calitatea de Operator de date cu caracter personal potrivit Regulamentului (UE) 679/2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date.

Denumirea: Institutul Oncologic "Prof. Dr. Ion Chiricuță", Cluj-Napoca.

Adresa: Mun. Cluj-Napoca, str. Republicii, nr. 34-36, RO400015, Cod fiscal 4547125, jud. Cluj.

Număr de telefon: 0264 598 361, 0264 598 362, 0264 598 363, 0264 598 364, 0264 591 281.

Adresă de e-mail: office@iocn.ro

Date de contact Responsabil de Protecția Datelor cu Caracter Personal: Tămaș-Bobocea Larisa-Ionela, adresă e-mail: dpo@iocn.ro.

Art. 2 Scopul și temeiul legal al prelucrării

Institutul Oncologic "Prof. Dr. Ion Chiricuță", Cluj-Napoca utilizează un sistem TVCI (televiziune cu circuit închis) în scopul asigurării pazei și protecției persoanelor, bunurilor și valorilor, al prevenirii și combaterii de contravenții sau infracțiuni, investigării eficiente a reclamațiilor, urmărind să descurajeze, detecteze sau împiedice orice încercare de pătrundere în obiectiv sau zona protejată.

Sistemul de supraveghere video nu este utilizat pentru verificarea prezenței angajaților la locul de muncă sau a modului de desfășurare a activității de către angajați. Cu toate acestea, dacă se ivește o posibilă cauză legată de un litigiu de dreptul muncii, înregistrările imaginilor, preluate în conformitate cu dispozițiile legale, pot fi utilizate pentru aflarea și stabilirea adevărului, respectând dispozițiile legale în vigoare.

Temeiul legal pentru prelucrarea imaginilor prin intermediul sistemului de supraveghere video este reglementat în Regulamentul (UE) 679/2016, **art. 6, alin. 1, lit. f)** "prelucrarea este necesară în scopul *intereselor legitime* urmărite de operator sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care

necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil”, cu respectarea dispozițiilor cuprinse în art. 5 din Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 679/2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date.

Interesul este *legal*. Astfel:

Potrivit Legii 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor se pot utiliza sisteme electronice de supraveghere video care să asigure paza și protecția persoanelor, bunurilor și valorilor, al prevenirii și combaterii de infracțiuni împotriva oricăror acțiuni ilicite care ar putea să aducă atingere dreptului la proprietate, dreptului la viață.

De asemenea, considerentul 47 din Regulamentul (UE) 679/2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal stabilește că: *”prelucrarea de date cu caracter personal strict necesară în scopul prevenirii fraudelor constituie, de asemenea, un interes legitim al operatorului de date în cauză”*, ceea ce justifică prelucrarea datelor cu caracter personal prin utilizarea mijloacelor de supraveghere video.

Interesul este *necesar*. Astfel:

Funcționarea unui sistem de supraveghere video pentru îndeplinirea scopurilor de mai sus este esențială întrucât, fiind vorba despre o instituție publică sanitară, unde fluxul de persoane este extrem de ridicat, folosirea oricăror alte mijloace mai puțin intruzive, de pildă: angajarea de personal care să verifice fiecare intrare din Institut, fiecare parcare, hol etc., ar fi inefficientă și insuficientă. Posibila anonimizare a înregistrărilor și estomparea fețelor persoanelor vizate ar face imposibilă identificarea persoanelor vizate în înregistrări și, prin urmare, scopul lor fundamental (protecția) nu ar putea fi atins. În plus, fără stocarea pentru o anumită perioadă de timp, înregistrările nu ar putea fi folosite ca dovezi sau ca mijloace de efectuare a controalelor.

Interesul este *specific*, fiind menționate scopurile exacte ale utilizării camerelor de supraveghere video.

Interesul este *real și actual*, întrucât posibilitatea încălcării scopului instalării mijloacelor de supraveghere video subzistă pe o perioadă nedeterminată de timp.

Art. 3 Drepturile persoanei vizate

Dreptul de acces la date. Aveți dreptul de a obține o confirmare că se prelucrează sau nu date cu caracter personal care vă privesc. Informațiile vă vor fi furnizate în termen de cel mult o lună de la primirea cererii, termen care poate fi prelungit cu încă 2 luni atunci când este necesar,

comunicându-vă și motivele întârzierii. Dacă perioada de stocare a imaginilor (20 de zile) s-a împlinit, informația pe care operatorul o comunică persoanei vizate este că nu mai sunt prelucrate date cu caracter personal. În situația în care în imaginile solicitate apar și alte persoane, se vor lua măsuri de editare a imaginilor: mascare, estomparea clarității, distorsionare, obturare. Pentru a putea fi furnizate informațiile solicitate, persoana vizată trebuie să se identifice prin prezentarea unui document de identitate și să menționeze data, ora locația și împrejurările în care a intrat în zona monitorizată video.

Dreptul la ștergerea datelor. Acest drept poate fi exercitat numai atunci când se aplică unul dintre motivele curpinse în art. 17, alin. 1 din Regulamentul GDPR și anume: datele nu mai sunt necesare pentru îndeplinirea scopurilor, v-ați retras consimțământul, dacă acesta a fost acordat, vă opuneți prelucrării, datele cu caracter personal au fost prelucrate ilegal, datele trebuie șterse pentru respectarea unei obligații legale care revine operatorului și datele au fost colectate în legătură cu oferirea de servicii ale societății informaționale. De asemenea, este necesară și inexistența unei situații excepționale regăsite la alin. 3 al aceluiași articol.

Dreptul la restricționarea prelucrării poate fi exercitat dacă dumneavoastră contestați exactitatea datelor, prelucrarea este ilegală, operatorul nu mai are nevoie de datele personale în scopul prelucrării, dar solicitați datele pentru constatarea, exercitarea sau apărarea unui drept în instanță sau dacă v-ați opus prelucrării.

Dreptul la portabilitatea datelor vă oferă posibilitatea de a primi datele care vă privesc și pe care ni le-ați furnizat și de a transmite aceste date altui operator.

Dreptul la opoziție poate fi exercitat atunci când vă opuneți prelucrării de date în scopul îndeplinirii unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investit operatorul sau dacă vă opuneți prelucrării de date necesare în interesele legitime ale operatorului.

Dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri.

Dreptul de a depune o plângere la Autoritatea Națională de Supraveghere a Protecției Datelor cu Caracter Personal atunci când considerați că v-au fost încălcate drepturile de către operator, după ce, în prealabil, s-au efectuat demersuri de comunicare directe cu noi în vederea soluționării amiabile a eventualelor diferende.

Dreptul de a depune o plângere la Autoritate se poate exercita prin accesarea site-ului https://www.dataprotection.ro/?page=Plangeri_pagina_principala. Datele de contact ale ANSPDCP sunt: B-dul G-ral Gheorghe Magheru, nr. 28-30, sector 1, cod poștal 010336, București, România, telefon: 40.318.059.211, anspdcp@dataprotection.ro.

Drepturile pot fi exercitate:

- prin completarea unui model de cerere publicat pe site-ul operatorului de date și trimis la adresa de e-mail: dpo@iocn.ro;
- prin transmiterea unei cereri la adresa de e-mail dpo@iocn.ro;
- prin poștă, la adresa Cluj-Napoca, str. Republicii, nr. 34-36, 400015, jud. Cluj;
- prin cerere scrisă depusă la Registratura generală de la sediul operatorului;
- verbal, cu condiția stabilirii identității persoanei solicitante.

Art. 4 Definiții

În **Anexa 1**, găsiți explicația termenilor utilizați în cuprinsul prezentei Politici privind supravegherea video.

Art. 5 Categoriile de date cu caracter personal pe care le prelucrăm

Imaginile sunt principalele date care se prelucrează prin intermediul sistemului de supraveghere video.

Nu prelucrăm date biometrice. Potrivit considerentului 51 din Regulamentul GDPR "prelucrarea fotografiilor nu ar trebui să fie considerată în mod sistematic ca fiind o prelucrare de categorii speciale de date cu caracter personal, întrucât fotografiile intră sub incidența definiției datelor biometrice doar în cazurile în care sunt prelucrate prin mijloace tehnice specifice care permit identificarea unică sau autentificarea unei persoane fizice."

Art. 6 Principiile prelucrării și securitatea datelor cu caracter personal

Institutul Oncologic "Prof. Dr. Ion Chiricuță", Cluj-Napoca prelucrează date cu caracter personal în conformitate cu prevederile Regulamentului GDPR și ale legislației naționale din sfera datelor cu caracter personal. Astfel, datele cu caracter personal vor fi:

- a) prelucrate în mod legal, echitabil și transparent față de persoana vizată („legalitate, echitate și transparență”);
- b) colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în interes public, în

scopuri de cercetare științifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile inițiale, în conformitate cu articolul 89 alineatul (1) („limitări legate de scop”);

c) adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate („reducerea la minimum a datelor”);

d) exacte și, în cazul în care este necesar, să fie actualizate; trebuie să se ia toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere („exactitate”);

e) păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele; datele cu caracter personal pot fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1), sub rezerva punerii în aplicare a măsurilor de ordin tehnic și organizatoric adecvate prevăzute în prezentul regulament în vederea garantării drepturilor și libertăților persoanei vizate („limitări legate de stocare”);

f) prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare („integritate și confidențialitate”).

Institutul Oncologic ”Prof. Dr. Ion Chiricuță”, Cluj-Napoca dispune măsurile tehnice și organizatorice conforme cu prevederile Regulamentului (UE) 679/2016 astfel că, procedurile de prelucrare pe care le efectuăm asigură confidențialitatea și securitatea datelor cu caracter personal.

Deși se iau toate măsurile pentru a asigura securitatea datelor dumneavoastră, Institutul Oncologic ”Prof. Dr. Ion Chiricuță”, Cluj-Napoca nu poate garanta lipsa oricărei încălcări de securitate sau intangibilitatea sistemelor de securitate. Dacă această situație se va ivi, vom pune în aplicare procedurile legale pentru limitarea efectelor și informarea persoanelor vizate.

Art. 7 Sistemul de supraveghere video

¹ Un sistem de supraveghere video (TVCI) este alcătuit din dispozitive analogice și digitale, precum și din software pentru captarea imaginilor unei scene, prelucrarea imaginilor și afișarea lor unui operator. Componentele sale sunt grupate în următoarele categorii:

¹ Pct. 9.1. din Ghidul 3/2019 privind prelucrarea datelor cu caracter personal prin mijloace video.

1. Mediul video: captarea imaginilor, interconectări și prelucrarea imaginilor:

- scopul captării imaginilor este generarea unei imagini a lumii reale într-un format în care să poată fi utilizată de restul sistemului;

- interconectările descriu toate transmisiile de date din mediul video, mai precis conectările și comunicațiile. Cablurile, rețelele digitale și transmisiile wireless reprezintă exemple de conectări. Comunicațiile descriu toate semnalele video și de date de control, care pot fi digitale sau analogice:

- prelucrarea imaginilor se referă la analiza, stocarea și prezentarea unei imagini sau a unei secvențe de imagini.

2. Din perspectiva gestionării sistemului, un TVCI are următoarele funcții logice:

- gestionarea datelor și a activităților, care include procesarea comenzilor operatorilor și a activităților generate de sistem (proceduri de alarmă, alertarea operatorilor);

- interfețe cu alte sisteme, printre care conectarea la alte sisteme de Securitate (controlul accesului, alarmă de incendiu) și fără legătură cu securitatea (sisteme de gestionare a clădirilor, recunoaștere automată a numărului de înmatriculare).

3. Securitatea TVCI constă în confidențialitatea, integritatea și disponibilitatea sistemului și a datelor:

- securitatea sistemului presupune securitatea fizică a tuturor componentelor sistemului și controlul accesului la TVCI;

- securitatea datelor se referă la prevenirea pierderii sau a manipulării datelor.

Administrarea și mentenanța sistemului de supraveghere video este asigurată de către administratorul societății S.C. SENTINEL ROMÂNIA S.R.L., str. Zaharia Bârsan, nr. 24, Cluj-Napoca, telefon: 0364 133 379, e-mail: sentinel.romania@gmail.com.

Camerele de supraveghere video sunt amplasate în locuri vizibile. Camerele nu sunt și nu vor fi montate în zone unde se impune asigurarea intimității persoanelor, cum ar fi: birouri, vestiare, toalete și alte locații similare.

Camerele amplasate astfel încât să înregistreze spațiile exterioare sunt poziționate în așa fel încât să prevină sau să minimizeze înregistrarea proprietății private sau înregistrarea trecătorilor. În funcție de rolul fiecărei camere, imaginile captate se limitează la o anumită arie de acoperire, iar datele cu caracter personal prelucrate sunt cele strict necesare pentru atingerea scopurilor sistemului de supraveghere.

Sunt instalate 120 de camere video fixe în interiorul și în exteriorul sediului operatorului, dintre care 3, sunt unități de înregistrare video de rețea. Toate camerele sunt funcționale 24 de ore timp de 7 zile pe săptămână.

Se supraveghează prin mijloace video:

- zonele de acces și intrările în sediul operatorului [intrarea de pe str. Ion Creangă; intrarea în parcare cu acces de pe str. Ion Creangă; intrarea dinspre blocurile ANL; intrarea dinspre parcare cu accesul de pe str. Republicii (parcarea de management); amfiteatrul spre magazia de alimente; intrarea în spălătorie; intrarea în farmacie; intrarea spital de zi; intrarea în bucătărie dinspre curtea interioară];

- holurile, casa scării;
- spațiile unde se află centrala termică, compresoarele;
- magazia;
- zona de spălătorie;
- zona de depozitare a deșeurilor;
- amfiteatre.

Art. 8 Perioada de stocare a imaginilor și ștergerea

Imaginile prelucrate prin mijloace de supraveghere video se stochează pe o perioadă de 20 de zile calendaristice. După împlinirea termenului, datele se șterg prin proces automat, începând cu cea mai veche înregistrare. Datele sunt stocate pe 4 hard disk-uri, amplasate în rack-uri, fiind închise într-o încăpere cu acces restricționat din cadrul Institutului Oncologic "Prof. Dr. Ion Chiricuță", Cluj-Napoca. În cazul producerii unui incident de securitate sau a unor investigații efectuate de către organele de urmărire penală, durata de stocare a imaginilor poate excede limita normală în funcție de timpul necesar pentru investigare.

Art. 9 Accesul la date

Datele pot fi accesate de către administratorul societății deținătoare a sistemului de supraveghere video, fiind singura persoană care are dreptul de acces în sistem. Orice altă persoană care solicită acces la imagini, trebuie să întocmească o cerere pe care o adresează managerului operatorului, urmând să fie analizat scopul accesului. Dacă acesta din urmă este unul legitim, se acordă acces asistat de către administratorul sistemului. De asemenea, imaginile prelucrate video se pot transmite, în condițiile legii, organelor judiciare, instanțelor de judecată sau altor autorități publice abilitate care, potrivit legii, au dreptul de a avea acces la aceste date.

Se va ține o evidență a datei oricărei divulgări, împreună cu detalii despre persoana căreia i-au fost furnizate acele informații, numele persoanei, motivul cererii, precum și modalitatea în care cererea a fost rezolvată, în cazul unei contestații. Atunci când se transmit imagini în care apar și alte persoane decât cele vizate, imaginile vor fi transmise după ce s-a estompat claritatea acelor părți din imagine în care apar și alte persoane, astfel încât să nu se aducă atingere drepturilor și libertăților acestora. În orice caz, fiecare activitate de dezvăluire a datelor cu caracter personal către terți va fi documentată și supusă unei analize complexe privind, pe de-o parte, necesitatea comunicării și, pe de altă parte, compatibilitatea dintre scopul în care se cere a se face comunicarea și scopul în care aceste date au fost prelucrate inițial. În aceste cazuri, va fi consultat Responsabilul de Protecția Datelor cu Caracter Personal.

În cazul unei anchete disciplinare, se pot accesa înregistrările din sistemul de supraveghere video, cu condiția ca informațiile să fie concludente și utile cauzei.

În locurile unde sunt montate monitoarele pe care pot fi vizualizate imaginile captate de camerele video, au acces personalul de la serviciul tehnic (3 persoane) și personalul care asigură paza și protecția (2 persoane). Aceștia au atribuția de a urmări imaginile și de a întocmi sesizări în cazul în care are loc un eveniment care pune în pericol protecția persoanelor, bunurilor/valorilor.

Art. 10 Măsuri tehnice și organizatorice

Pentru a proteja securitatea datelor cu caracter personal colectate sunt stabilite următoarele măsuri tehnice și organizatorice:

- a) limitarea timpului de stocare a imaginilor prelucrate prin intermediul sistemului de supraveghere video;
- b) spațiile de stocare a imaginilor se află în încăperi securizate, unde au acces doar persoane autorizate;
- c) accesul la date este limitat, având acest drept numai administratorul societății deținătoare a sistemului;
- d) persoana care hotărăște cine are drept de acces la imagini (cu excepția persoanei vizate care își poate exercita dreptul de acces conform Capitolului II) este managerul Institutului;
- e) păstrarea unui Registru de acces la datele obținute prin sistemul de supraveghere video;
- f) revizuirea periodică în scopul reanalizării necesității menținerii în uz a sistemului, îndeplinirii scopului declarat.

Art. 11 Transparența informațiilor

Locația camerelor de supraveghere va fi indicată prin pictograme. La fiecare intrare principală în sediul operatorului, pictogramele afișate vor conține următoarele informații: datele de contact ale operatorului, scopurile prelucrării și drepturile persoanei vizate.

Prezenta Politică poate fi accesată pe site-ul <http://www.iocn.ro> sau se poate solicita o copie la adresa de e-mail dpo@iocn.ro ori de la Registratura generală.

Această informare poate fi revizuită ori de câte ori considerăm necesar, urmând să fie adusă la cunoștința persoanelor vizate.

Anexa 1- Definiții

a) „date cu caracter personal” înseamnă orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată”); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;

b) „prelucrare” înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;

c) „operator” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern;

d) „persoană împuternicită de operator” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului;

e) „consimțământ” al persoanei vizate înseamnă orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;

f) „supraveghere TVCI” înseamnă sistem de televiziune cu circuit închis/supraveghere video;

g) „persoana vizată” înseamnă orice persoană fizică ale cărei date sunt prelucrate;

j) ”ANSPDCP” Autoritatea Națională de Supraveghere a Protecției Datelor cu Caracter Personal;

m) ”măsuri tehnice și organizatorice” înseamnă măsurile de securitate luate de către operator cu privire la prelucrarea datelor cu caracter personal.

Art. 12 Prezenta Decizie este adusă la cunoștința persoanelor vizate prin transmitere electronică, la adresele de e-mail și/sau prin publicarea pe Intranet și/sau website-ul operatorului.

Art. 13 Prezenta Decizie este valabilă până la revocare sau înlocuire ulterioară.

Manager

Director medical

Director de îngrijiri

Consilier juridic

Responsabil de Protecția Datelor cu Caracter Personal