

NOTĂ DE INFORMARE PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL ȘI POLITICA PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL

În conformitate cu dispozițiile Regulamentului (UE) nr. 2016/679 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, cunoscut sub denumirea de „Regulamentul General privind Protecția Datelor” sau, pe scurt, „RGPD”, vă aducem la cunoștință următoarele aspecte legate de prelucrarea datelor dumneavoastră cu caracter personal:

1. Cine este operatorul datelor cu caracter personal?

INCARMED S.R.L., persoană juridică română, cu sediul social în Calimanesti, str. Calea lui Traian nr. 734, înregistrată la Oficiul Registrului Comerțului de pe lângă Tribunalul Valcea sub nr. J38/505/2005, CUI 17645176, Tel: 0731.371.371.

2. Ce date cu caracter personal prelucrăm?

În cazul în care sunteți pacient INCARMED:

- **Informații generale (date de identificare):** nume, prenume, data nașterii, sex, naționalitate, vârstă, CNP, adresa de domiciliu sau de reședință, e-mail, telefon, ID pacient, loc de muncă (dacă este cazul), calitatea de abonat (dacă este cazul), copie certificat de naștere, copie C.I., semnătura, iar în cazul în care veți fi internat, datele de identificare ale aparținătorului (nume, prenume, grad de rudenie, telefon);
- **Date privind situația debitelor:** istoric financiar în cadrul Incarmed, situația plăților restante;
- **Date de sănătate sau conexe prestării serviciilor medicale:**
- **Date generale:** greutate, înălțime, calitatea de fumător ori nefumător, grupă sanguină, RH, istoric medical, scrisori medicale, alergii, simptomatologie, diagnostic, antecedente (heredocolaterale, fiziologice și patologice), tipul intervenției, acte ce țin de activitatea medicală, cum ar fi: recomandare medic familie ori medic specialist, raport medical, cod diagnostic, tipul de program prin care vine pacientul (management boală cronică/acută), semnătura pacientului, calitatea de asigurat CNAS sau de asigurat în sistemul privat (în cazul societăților de asigurări private de sănătate), nr. card de sănătate, card de identificare oferit de compania asigurătoare (după caz), bilet de trimitere, foaia de observație, decont cheltuieli și documente medicale din timpul spitalizării (după caz), investigații efectuate, ziua și ora internării, rezervă și pat pacient (în cazul în care veți fi internat), bilet externare, ora și ziua externării, ziua/ora/locația recoltării probelor, diagnostic prezumtiv, informații evoluție stare de sănătate, alergii, medicație prescrisă pentru diverse patologii, informații medicale în urma realizării consultului, talon pensie (după caz);
- **Date privind spitalizarea:** bilet de trimitere, foaia de observație, decont cheltuieli și documente medicale din timpul spitalizării, investigații efectuate, ziua și ora internării, rezervă și pat alocat, observații pacient cu privire la vizite, evoluția pacientului pe perioada spitalizării, bilet externare, ora și ziua externării, diagnostic prezumtiv, alergii, medicație prescrisă pentru diverse patologii, informații medicale în urma realizării consultului, talon pensie (după caz), nume, prenume și specialitate medic curant (după caz), nume, prenume, grad de rudenie și telefon aparținător;
- **Date privind analizele:** data și ora programării, date privind consultațiile și analizele, data, ora și locația recoltării, codul de probă., rezultate analize.

În cazul în care vrei să faci parte din echipa INCARMED:

- **Date privind procesul de recrutare:** nume, prenume, vârstă, sex, naționalitate, adresă de domiciliu ori de reședință, datele cuprinse în CV, carnet de muncă (după caz), nivelul și specializarea studiilor impuse de cerințele postului; documente de suport care includ și date sensibile, cum ar fi cazierul judiciar, caracterizarea de la ultimul loc de muncă (după caz),

În cazul în care ne vei vizita la sediul nostru:

- **Date privind imaginea:** imagine video captată prin intermediul camerelor de supraveghere amplasate în locuri vizibile în locație;

În cazul în care accesezi website-ul INCARMED:

- **Date referitoare la profilarea utilizatorilor website-ului INCARMED:** vârsta, sex, IP, date de trafic, date de geo-localizare, dispozitiv utilizat, sistem operare, cuvinte cheie căutate de utilizator conform intereselor sale.

3. De unde obținem datele cu caracter personal?

Ca regulă, datele cu caracter personal pe care le prelucrăm sunt obținute în mod direct de la dumneavoastră în momentul efectuării programărilor ori al prestării serviciilor medicale solicitate. Însă, există și situații în care vom intra în posesia datelor dumneavoastră cu caracter personal prin intermediul altor mijloace legale și, totodată, legitime, cum ar fi executarea unui contract la care dumneavoastră nu sunteți parte în mod direct.

În cazul în care beneficiați de asigurări medicale private, în funcție de contractul încheiat cu fiecare asigurător în parte, asigurătorul dumneavoastră ne va transmite datele cu caracter personal necesare luării în evidență ca având calitatea de asigurat.

4. Care sunt scopurile prelucrării datelor cu caracter personal?

Datele dumneavoastră cu caracter personal sunt prelucrate de către INCARMED în scopuri legitime legate de prestarea serviciilor medicale, conform reglementărilor legale în vigoare, după cum urmează:

- Încheierea și executarea contractelor de prestare servicii medicale pentru pacientul adult,
- Efectuarea programărilor în unitățile medicale INCARMED sau telefonic, în vederea realizării actului medical conform nevoilor pacienților, a analizelor medicale, în vederea stabilirii diagnosticului, în scopul internării pacienților pentru intervenții/investigații și externare; eliberării de rețete medicale, acordării concediilor medicale, precum și alte servicii medicale conform situației specifice fiecărui pacient în parte, precum și pentru întocmirea și ținerea evidențelor programărilor și a bazei de date a pacienților în sistemele IT (tehnologia informației);
- Gestionarea sistemelor de comunicații și a sistemelor IT, efectuarea de rapoarte de audit, gestionarea securității bazelor de date și a tuturor sistemelor IT;
- Efectuarea decontării serviciilor către Casele de Asigurări de Sănătate sau de către asiguratorul extern (după caz);
- Întocmirea documentelor fiscale și încasarea sumelor de plată de la pacienți persoane fizice, inclusiv recuperarea debitelor și a facturilor emise de furnizori și realizarea plății acestora;
- Raportarea prin corespondență sau prin e-mail către Serviciul de Prevenire a Infecțiilor Asociate Asistenței Medicale (SPIAAM) și către Direcția de Sănătate Publică (DSP), în vederea depistării anumitor infecții ale pacienților, respectiv pentru ținerea registrului electronic unic de monitorizare a infecțiilor asociate asistenței medicale al unității;
- Soluționarea cererilor și adreselor instituțiilor publice în legătură cu pacienții, în baza unor dispoziții legale imperative, dacă este cazul;
- Organizarea gărzilor, a raportărilor, realizarea evidenței serviciilor medicale, evidența programărilor în aplicațiile IT, soluționarea reclamațiilor și cererilor primite din partea pacienților sau altor persoane vizate, gestionarea corespondenței uzuale, verificării gradului de ocupare pe saloane, întocmirii fișelor de consum, controlului accesului vizitatorilor în saloane, întocmiri de procese-verbale pentru predare-primire bunuri ale pacienților, redactare registru analize pacienți;
- Asigurarea pazei bunurilor și a persoanelor în interiorul locațiilor INCARMED prin utilizarea sistemului de supraveghere video;
- Reprezentarea societății în fața instanțelor de judecată și a autoritatilor publice, realizarea procedurilor de recuperare a creanțelor, după caz;
- Desfășurarea activităților de recrutare/selecție pentru ocuparea posturilor vacante și gestionarea dosarelor de recrutare/concurs în diferitele etape ale procedurilor de recrutare/selecție, în vederea organizării examenului/concursului de ocupare a postului vacant;

ATENȚIE! În cazul în care INCARMED va dori să prelucreze datele dumneavoastră cu caracter personal în alte scopuri decât cele declarate inițial, vi se va transmite o notă de informare separată, în care vi se va detalia scopul ulterior al prelucrării, temeiul juridic al prelucrării, precum și perioada de stocare a datelor dumneavoastră cu caracter personal, împreună cu orice alte informații utile în legătură cu prelucrările ulterioare pentru a vă permite

să vă exprimați consimțământul în mod liber, în cunoștință de cauză și în mod expres pentru fiecare operațiune de prelucrare în parte (dacă prelucrarea respectivă este condiționată de obținerea consimțământului expres al dumneavoastră).

5. **Care sunt temeiurile juridice ale prelucrării datelor cu caracter personal?**

- **Efectuarea de demersuri la cererea dumneavoastră** înainte de încheierea unui contract (art. 6 alin. (1) lit. b) teza a II-a din RGPD);
- **Executarea contractelor de prestări servicii medicale**, la care pacienții sunt parte (art. 6 alin. (1) lit. b) teza I din RGPD);
- **Îndeplinirea unor obligații legale** de către Incarmed (art. 6 alin. (1) lit. c) din RGPD);
- **Protejarea intereselor dumneavoastră vitale**, în situația în care vă aflați, spre exemplu, într-o situație de urgență medicală sau în vederea protejării intereselor vitale ale altor persoane fizice (art. 6 alin. (1) lit. d) din RGPD);
- **Interesul legitim al INCARMED** (art. 6 alin. (1) lit. f) din RGPD), cum ar fi: organizarea întregii activități a Incarmed pentru îndeplinirea obiectului de activitate; identificarea pacienților în momentul prezentării la recepție pentru programare sau urgență medicală; organizarea gărzilor și a predării acestora; evidența serviciilor medicale; evidența programărilor în aplicațiile IT; soluționarea reclamațiilor și a cererilor primite din partea pacienților sau altor persoane vizate; controlul accesului vizitatorilor în saloane; demararea și desfășurarea litigiilor pe rolul instanțelor de judecată și (eventual) al altor autorități publice; proceduri de recuperare a creanțelor;
- **Consimțământul dumneavoastră** pentru prelucrare, atunci când este acordat expres, liber și necondiționat, în situații punctuale cum ar fi, spre exemplu, prelucrările în scop de marketing (art. 6 alin. (1) lit. a) din RGPD).

Pentru **categoriile speciale de date** prelucrate (**datele privind sănătatea**), temeiurile prelucrării sunt următoarele:

- Scopuri legate de medicina preventivă sau a muncii, de evaluare a capacității de muncă a angajatului, de stabilire a unui diagnostic medical, de furnizare de asistență medicală sau socială sau a unui tratament medical sau de gestionare a sistemelor și serviciilor de sănătate ori de asistență socială (art. 9 alin. (2) lit. h) din RGPD);
- Motive de interes public în domeniul sănătății publice (art. 9 alin. (2) lit. i) din RGPD);
- Protejarea intereselor vitale ale dumneavoastră sau ale unei alte persoane fizice, atunci când persoana în cauză se află în incapacitate fizică sau juridică de a-și da consimțământul la prelucrare (art. 9 alin. (2) lit. c) din RGPD);
- Constatarea, exercitarea sau apărarea unui drept în instanță (art. 9 alin. (2) lit. f) din RGPD), în caz de litigiu. Exemplificare conform tabel:

Prelucrare date de natura personala	Condiții prevazute în regulament
Prelucrarea datelor necesare pentru procesul de recrutare, primite direct de la candidați sau prin intermediul site-urilor de recrutare	Art.6(1)a, persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice.
Prelucrarea datelor angajaților necesară pentru îndeplinirea condițiilor contractuale dintre Incarmed SRL și angajați. Prelucrarea categoriilor sensibile de date este necesară pe baza faptului că organizația își îndeplinește obligațiile legale și prelucrează date legate de medicina muncii sau de evaluarea capacității de muncă a angajatului.	Art.6(1)b, pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract, Art.6(1)c, îndeplinirea unei obligații legale, Art.9(2)h, date legate de medicina muncii sau de evaluarea capacității de muncă a angajatului
Monitorizarea accesului, a email-urilor și a traficului de internet pentru a asigura siguranța și securitatea sistemelor informatice ale spitalului.	Art.6(1)f, prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terță.
Fotografii sau înregistrări video realizate pentru prezentarea condițiilor și serviciilor oferite	Art.6(1)a, persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice.

Supraveghere video folosind sistemul intern de supraveghere video pentru a asigura siguranța și securitatea angajaților și bunurilor spitalului.	Art.6(1)c, în vederea îndeplinirii unei obligații legale, Art.6(1)f, prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terță.
--	--

6. Pentru ce perioadă sunt prelucrate datele cu caracter personal?

În cadrul scopurilor legate de activitatea INCARMED, datele dumneavoastră cu caracter personal vor fi stocate pe o perioadă limitată de timp într-un loc sigur și în conformitate cu condițiile și prevederile legale în domeniu, astfel:

- Datele dumneavoastră care sunt necesare în scopuri legate de serviciile medicale vor fi stocate pe durata contractului de prestări servicii medicale, respectiv pentru o perioadă de timp rezonabilă, după încetarea contractelor, inclusiv perioada de timp necesară în vederea îndeplinirii obligațiilor legale prevăzute de legislația aplicabilă, constând într-o perioadă generală de 50 de ani, cu excepția cazului în care pentru anumite documente medicale necesare sunt impuse termene de stocare mai mari ori mai scurte;
- Datele prelucrate în scopuri contabile, în special cele legate de facturare și plăți, vor fi stocate pe o perioadă de 10 ani, cu începere de la data de 1 ianuarie a anului următor încheierii exercițiului financiar în cursul căruia au fost întocmite, conform prevederilor Legii contabilității nr. 82/1991, cu modificările și completările ulterioare, inclusiv cele aduse prin Legea nr. 163/2018;
- Datele privind supravegherea video pentru asigurarea securității bunurilor și persoanelor, respectiv a înregistrării apelurilor telefonice și a opiniei dumneavoastră privind serviciile INCARMED se vor stoca pe o perioadă de 30 de zile calendaristice, respectiv în conformitate cu temeiurile prevăzute de legislația aplicabilă în vigoare;
- Datele privind procesul de recrutare vor fi păstrate pe o perioadă de 6 luni de la momentul încheierii procesului de recrutare/selecție pentru postul vacant pentru care ați candidat.

În situația în veți decide să vă retrageți consimțământul acordat pentru prelucrarea datelor dumneavoastră în scopuri legate de marketing-ul direct, datele dumneavoastră cu caracter personal nu vor mai fi prelucrate în acest scop, din momentul retragerii consimțământului, fără a afecta însă valabilitatea prelucrării datelor efectuată înainte de acest moment:

- De asemenea, datele dumneavoastră cu caracter personal vor fi prelucrate și pe durata existenței unor obligații legale de păstrare a anumitor categorii de date ori de documente justificative, în funcție de reglementările în vigoare, în special în domeniul sănătății publice ori în domeniul fiscal.

7. Căror entități vom divulga datele dumneavoastră cu caracter personal?

În anumite condiții expres reglementate, datele dumneavoastră cu caracter personal pot fi prelucrate de către INCARMED, prin intermediul unor Persoane împuternicite ori în comun cu alte societăți, în acest din urmă caz, fiind vorba despre o relație de tipul operatori asociați, care vor stabili în comun scopurile și mijloacele de prelucrare, conform dispozițiilor art. 26 din RGPD.

În unele situații, vor putea avea acces la datele dumneavoastră cu caracter personal furnizorii de servicii cum ar fi, dar fără a se limita la furnizorii de servicii și sisteme IT, diverși partenerii contractuali cum ar fi: Softeh Plus, ș.a. De asemenea, se vor putea transmite datele dumneavoastră către avocați, contabili, auditori sau alți profesioniști care au obligația păstrării secretului profesional.

În vederea asigurării serviciilor medicale complete, datele dumneavoastră vor fi furnizate medicilor colaboratori ori laboratoarelor partenere, cu care există încheiate acorduri de confidențialitate.

Pentru raportările către autoritățile statului, potrivit obligațiilor legale în vigoare, va fi necesară transmiterea datelor dumneavoastră către diverse instituții publice, cum ar fi, spre exemplu: Casa Națională de Asigurări de Sănătate (CNAS), SNSPMS.

În cazul în care sunteți asigurat la o companie privată de asigurări de sănătate din România ori din alt stat european, datele dumneavoastră cu caracter personal vor fi transmise către asigurător, în vederea decontării serviciilor medicale de care ați beneficiat.

8. Cum și când se realizează transferul datelor dumneavoastră cu caracter personal către țări terțe?

Datele cu caracter personal pot fi transferate în afara Uniunii Europene în anumite circumstanțe. GDPR enumeră factorii care ar trebui luați în considerare pentru a asigura un nivel adecvat de protecție a datelor și câteva scutiri în baza cărora pot fi exportate datele. În toate cazurile, INCARMED S.R.L. va solicita consimțământul persoanelor vizate înainte ca informațiile cu caracter personal să poată fi transferate în afara UE.

9. Care sunt drepturile dumneavoastră în legătură cu prelucrarea datelor cu caracter personal?

În ceea ce privește prelucrarea datelor dumneavoastră cu caracter personal, în temeiul art. 15-22 din RGPD, vă sunt garantate o serie de drepturi:

- **dreptul de acces** la date – presupune posibilitatea formulării unei cereri prin care puteți obține confirmarea faptului că vă sunt prelucrate date cu caracter personal și prin care puteți avea acces la categoriile de date prelucrate și informații suplimentare referitoare la prelucrările efectuate, ori, după caz, puteți solicita o copie a datelor cu caracter personal care fac obiectul prelucrării;
- **dreptul la rectificare** – puteți obține, fără întârzieri nejustificate, corectarea (rectificarea) datelor inexacte pe care le prelucram în legătură cu dumneavoastră;
- **dreptul la ștergerea datelor** (denumit și „*dreptul de a fi uitat*”, în mediul on-line) – constă în posibilitatea solicitării și obținerii ștergerii datelor cu caracter personal, în măsura în care dispozițiile legale în vigoare permit acest lucru;
- **dreptul la restricționarea prelucrării** – veți avea posibilitatea de a obține restricționarea prelucrării, numai în situațiile expres prevăzute de lege;
- **dreptul la portabilitatea datelor** – veți putea primi datele dumneavoastră cu caracter personal într-un format structurat, astfel încât să se poată face transferul acestora către un alt operator, în mod automat;
- **dreptul la opoziție** – presupune faptul că vă puteți opune prelucrării datelor dumneavoastră cu caracter personal în anumite situații și doar în cazul în care prelucrarea în cauză are ca temei îndeplinirea unei sarcini de interes public ori se bazează pe interesul legitim al operatorului;
- **dreptul de a nu fi supus unei decizii individuale automatizate** – înseamnă ca aveți dreptul de a solicita și de a obține retragerea, anularea și reconsiderarea oricărei decizii care produce efecte juridice asupra dumneavoastră, adoptată exclusiv în baza unei operațiuni de prelucrare a datelor cu caracter personal prin mijloace automatizate, în scopul evaluării unor trăsături de personalitate, precum abilitățile profesionale, credibilitatea, comportamentul dumneavoastră la locul de muncă, interesele ș.a..

Disponibilitatea drepturilor depinde în mare măsură de justificarea legală a prelucrării. Tabelul următor rezumă momentul în care drepturile sunt disponibile.

Drepturi persoana vizată	Baze legale prelucrare					
	Consimțământ	Contract	Obligație legală	Interes vital	Interes public	Interes Legitim
Retragere consimțământ	Da	Nu	Nu	Nu	Nu	Nu
Informare	Da	Da	Da	Da	Da	Da
Acces	Da	Da	Da	Da	Da	Da
Corectare	Da	Da	Da	Da	Da	Da
Ștergere	Da	Nu	Nu	Nu	Nu	Da
Restricționare procesare	Da	Da	Da	Da	Da	Da
Portabilitate date	Da	Da	Nu	Nu	Nu	Nu
Obiecție	-	Nu	Nu	Nu	Da	Da
Decizii automate și profilare	-	Nu	Nu	Da	Da	Da

Orice solicitări făcute pentru a invoca oricare dintre drepturile anterioare trebuie tratate prompt și, în orice caz, în termen de o lună de la primirea cererii. Personalul trebuie să consulte responsabilul pentru protecția datelor dacă sunt primite cereri de acest fel.

Nu în ultimul rând, vă aducem la cunoștință faptul că aveți **dreptul de a vă adresa Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)** sau oricărei instanțe competente în domeniul protecției datelor cu caracter personal.

Pentru a vă exercita aceste drepturi, puteți contacta **Incarmed SRL** printr-o solicitare scrisă, datată și semnată, transmisă în atenția Responsabilului cu protecția datelor cu caracter personal din cadrul **Incarmed SRL** la adresa de corespondență menționată la pct. 10 sau prin e-mail la adresa dpo@sicc.ro.

Solicitarea dumneavoastră va fi analizată cu maximă atenție și vi se va transmite un răspuns în termenul legal de 30 de zile calendaristice de la primirea solicitării, conform prevederilor RGPD. În cazul în care solicitarea dumneavoastră presupune o cercetare minuțioasă datorită complexității cererii, termenul de o lună poate fi prelungit cu încă o lună, însă vi se vor transmite argumentele necesității prelungirii termenului de soluționare.

Responsabilul cu protecția datelor

Spitalul este obligat să desemneze un Responsabil cu protecția datelor (DPO). Responsabilul cu protecția datelor poate fi un angajat din cadrul organizației, îndeplinind sarcinile în baza unui contract individual de muncă sau poate fi un colaborator extern, îndeplinindu-și sarcinile în baza unui contract de prestări servicii. Detalii în Procedura de desemnare a Responsabilului cu protecția datelor.

Rolul Responsabilului cu protecția datelor este de a asigura în mod independent aplicarea corectă a normelor de protecție a datelor în cadrul Spitalului. Astfel, acesta contribuie la protecția drepturilor și a libertăților persoanelor fizice ale căror date cu caracter personal sunt prelucrate de către organizație.

În acest scop, Responsabilul cu protecția datelor:

- sporește gradul de cunoaștere cu privire la obligațiile în materie de protecție a datelor;
- oferă consiliere personalului cu privire la protecția datelor;
- semnalează nerespectarea normelor aplicabile.

În afară de rolul consultativ general al Responsabilului cu protecția datelor, acesta poate efectua investigații, în mod voluntar sau la cerere, cu privire la chestiuni legate de protecția datelor.

10. Cum pot lua legătura cu Responsabilul cu protecția datelor din cadrul Incarmed SRL?

Datele de contact ale Responsabilului cu protecția datelor cu caracter personal din cadrul Incarmed SRL sunt următoarele: Adresa de corespondență: Calimanesti, str. Calea lui Traian nr. 734. Adresa de email: dpo@sicc.ro.

11. Ce înțeles au termenii utilizați în cuprinsul prezentei note de informare?

Date cu caracter personal – orice informații în legătură cu o persoană fizică identificată sau identificabilă. Va fi considerată identificabilă acea persoană fizică ce va putea fi identificată în mod direct ori indirect, în special prin utilizarea unui element de identificare, cum ar fi, spre exemplu, un identificator online;

Categorii speciale de date cu caracter personal – date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă, convingerile filozofice ori apartenența la sindicate, viața sexuală ori orientarea sexuală, datele privind condamnările penale, date genetice, date biometrice, date privind sănătatea;

Date privind sănătatea – datele cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistență medicală, care dezvăluie informații despre starea de sănătate a acesteia;

Consimțământ – 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;

Prelucrarea datelor cu caracter personal – orice operațiune sau set de operațiuni efectuate în legătură cu datele cu caracter personal, cu sau fără utilizarea de mijloace automatizate cum ar fi, spre exemplu, colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea, modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;

Operator de date cu caracter personal – persoană fizică sau juridică, precum și orice autoritate publică, agenție sau alt organism care, singur ori împreună cu altele stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal;

Persoană împuternicită – persoana fizică sau juridică, autoritatea publică, agenție sau alt organism care prelucrează datele cu caracter personal în numele operatorului;

Persoana vizată – persoana fizică ale cărei date cu caracter personal sunt prelucrate de către operator ori de persoana împuternicită de operator;

Țară terță – țară aflată înafara Uniunii Europene ori Spațiului Economic European.

12. Site-uri web

Site-ul web al Spitalului trebuie să se supună regulilor stabilite la nivelul organizației din punct de vedere al aspectului, securității și al protecției datelor cu caracter personal.

Pentru conformarea la cerințele GDPR, pe site-ul web se vor aplica cel puțin următoarele măsuri tehnice:

- postarea unei informări cu privire la cookie-urile utilizate de site-ul web și modul în care utilizatorul poate să se opună instalării acestora;
- postarea unei informări privind confidențialitatea care să cuprindă denumirea operatorului, scopul prelucrării, datele prelucrate, posibilele transferuri internaționale, drepturile de care beneficiază persoana vizată ș.a.m.d.;
- în cazul în care se dorește utilizarea datelor de contact și în alte scopuri (comunicări de marketing, newsletter ș.a.m.d.) includerea unei informări și a unei forme de preluare a consimțământului utilizatorului și de retragere a acestuia;
- asigurarea unor măsuri tehnice pentru protecția datelor cu caracter personal transmise de către utilizator.

13. Încălcarea confidențialității datelor cu caracter personal

Spitalul este responsabil de asigurarea unei securități adecvate și proporționale a datelor personale pe care le deține. Aceasta include protejarea datelor împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, distrugerii sau deteriorării accidentale a datelor. Spitalul depune toate eforturile pentru a evita încălcarea datelor cu caracter personal, totuși, este posibil ca greșelile să apară ocazional. Exemple de încălcări ale datelor cu caracter personal includ:

- Pierderea sau furtul de date sau echipamente ce conțin date cu caracter personal;
- Controale de acces necorespunzătoare care să permită utilizarea neautorizată;
- Probleme ale echipamentelor ce permit accesul neautorizat;
- Dezvăluirea neautorizată (de exemplu, e-mail-urile trimise destinatarului incorect);
- Eroarea umană;
- Hacking.

Dacă se observă o încălcare a protecției datelor, trebuie raportată imediat. Detalii privind modul de raportare a unei încălcări și informațiile care vor fi solicitate, sunt incluse în Procedura privind managementul încălcărilor securității datelor cu caracter personal.

În anumite cazuri de încălcare a protecției datelor, Spitalul este obligat să raporteze acest lucru, cât mai curând posibil, Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), dar nu mai târziu de 72 de ore de la constatarea acesteia.

Detalii privind modul de raportare a unei încălcări către ANSPDCP sunt incluse în Procedura de notificare a încălcării confidențialității datelor.

14. Impactul nerespectării

Toți angajații Spitalului sunt obligați să respecte această politică de protecție a datelor, îndrumările sale și cerințele specificate în GDPR. Orice membru al personalului care a divulgat neautorizat informații cu caracter personal sau a încălcat termenii acestei Politici poate face obiectul unor măsuri disciplinare.

Spitalul ar putea fi amendat pentru nerespectarea GDPR. Amenzile sunt diferențiate în funcție de încălcarea obligațiilor operatorului, ale persoanei împuternicite de operator ș.a.m.d. sau de încălcarea principiilor de bază pentru prelucrare, inclusiv a condițiilor privind consimțământul, a drepturilor persoanelor vizate ș.a.m.d.

15. Responsabilități

15.1. Management organizație

Managementul are următoarele responsabilități:

- a) aprobă politica generală, politicile subsecvente și obiectivele privind protecția datelor cu caracter personal,
- b) se asigură că sunt disponibile resursele necesare implementării măsurilor tehnice și organizatorice de protecție a datelor și de respectare a drepturilor persoanelor vizate,
- c) desemnează un Responsabil cu protecția datelor și se asigură că acesta are competențele necesare,
- d) se asigură că Responsabilul cu protecția datelor este implicat în mod corespunzător și în timp util în toate aspectele legate de protecția datelor cu caracter personal,
- e) se asigură că Responsabilul cu protecția datelor nu primește niciun fel de instrucțiuni în ceea ce privește îndeplinirea sarcinilor atribuite,
- f) comunică importanța respectării cerințelor Regulamentului UE 679 /2016 – GDPR.

15.2. Responsabilul cu protecția datelor

Responsabilul cu protecția datelor răspunde direct în fața Managementului Spitalului.

Responsabilul cu protecția datelor are cel puțin următoarele responsabilități:

- a) informează și oferă consiliere personalului Spitalului și persoanelor împuternicite de organizație pentru prelucrarea datelor cu caracter personal care își desfășoară activitatea în temeiul GDPR și al altor dispoziții naționale sau ale Uniunii Europene privind protecția datelor,
 - b) coordonează identificarea și evaluarea activităților de prelucrare a datelor desfășurate în organizație,
 - c) participă la întâlniri cu conducerea organizației, atunci când sunt concepute noi prelucrări, pentru a se asigura de respectarea principiului protecției datelor începând cu momentul conceperii, la toate nivelurile,
 - d) menține evidențele activităților de prelucrare în conformitate cu articolul 30 din GDPR,
 - e) monitorizează conformitatea cu GDPR, cu alte dispoziții naționale sau ale Uniunii Europene privind protecția datelor și cu politicile și procedurile Spitalului în ceea ce privește protecția datelor cu caracter personal, inclusiv atribuirea responsabilităților, conștientizarea și instruirea personalului implicat în operațiunile de prelucrare și auditurile aferente,
 - f) oferă consiliere atunci când este solicitat în ceea ce privește evaluarea impactului asupra protecției datelor (DPIA) și monitorizează performanța sa în conformitate cu articolul 35,
 - g) cooperează cu autoritatea de supraveghere,
 - h) întocmește și actualizează politicile și procedurile interne de protecție a datelor,
 - i) efectuează audituri pentru a determina conformitatea cu politicile și procedurile interne de protecție a datelor și necesitățile de îmbunătățire,
 - j) implementează un program de instruire cu privire la protecția datelor personale pentru personalul Spitalului implicat în activități de prelucrare,
 - k) urmărește modificările aduse legislației și formulează recomandări pentru a asigura conformitatea cu aceste modificări,
 - l) menține o evidență a încălcărilor vieții private în operațiunile de prelucrare desfășurate de organizație,
 - m) oferă consiliere cu privire la modul de abordare a încălcărilor vieții private,
 - n) se asigură că organizația răspunde solicitărilor persoanelor vizate în termenele legale,
 - o) acționează ca punct de contact cu rezidenții din UE, autoritatea de supraveghere națională și autoritățile celorlalte țări ale Uniunii Europene și cu echipele interne în ceea ce privește aspectele legate de prelucrare, inclusiv consultarea prealabilă menționată la articolul 36 și consultă autoritatea de supraveghere națională, dacă este cazul, cu privire la orice altă chestiune,
 - p) are obligația de a respecta secretul sau confidențialitatea în ceea ce privește îndeplinirea sarcinilor sale.
- În îndeplinirea atribuțiilor sale, Responsabilul cu protecția datelor are în vedere riscurile asociate operațiunilor de prelucrare, ținând seama de natura, de domeniul de aplicare, de contextul și de scopurile procesării.

15.3. Șefi departamente

Șefii de departamente sunt responsabili pentru:

- a) implementarea de zi cu zi a cerințelor privind gestionarea în siguranță a datelor cu caracter personal,

- b) asigurarea că măsurile de securitate tehnice, fizice și organizatorice stabilite sunt aplicate în mod corespunzător și de către tot personalul,
- c) asigurarea resurselor și efectuarea analizelor necesare pentru a se asigura că informațiile și activele informaționale sunt protejate în mod corespunzător în zona lor de responsabilitate,
- d) informarea Responsabilului cu protecția datelor despre încălcările reale sau presupuse ale politicilor de confidențialitate a datelor din zona lor de responsabilitate (incidente privind confidențialitatea datelor).

15.4. Personalul implicat în prelucrări

Personalul implicat în prelucrări are următoarele responsabilități:

- a) respectă toate politicile privind confidențialitatea și protecția datelor aplicabile pentru locurile lor de muncă,
- b) sunt responsabili pentru menținerea protecției și confidențialității tuturor informațiilor încredințate,
- c) informează Managementul organizației/sefi departamente despre încălcările reale sau presupuse ale politicilor de confidențialitate a datelor din zona lor de responsabilitate (incidente privind confidențialitatea datelor).

15.5. Personalul neimplicat direct în prelucrări

Personalul neimplicat direct în prelucrări are următoarele responsabilități:

- a) respectă toate politicile privind confidențialitatea și protecția datelor aplicabile pentru locurile lor de muncă,
- b) informează Managementul organizației / sefi departamente despre încălcările reale sau presupuse ale politicilor de confidențialitate a datelor din zona lor de responsabilitate (incidente privind confidențialitatea datelor).

15.6. Colaboratori

Colaboratorii implicați în prelucrări au următoarele responsabilități:

- a) respectă toate politicile privind confidențialitatea și protecția datelor aplicabile pentru prelucrările de date cu caracter personal efectuate,
- b) sunt responsabili pentru menținerea protecției și confidențialității tuturor informațiilor încredințate,
- c) informează Șefii entităților organizatorice despre încălcările reale sau presupuse ale politicilor de confidențialitate a datelor din zona lor de responsabilitate (incidente privind confidențialitatea datelor).

15.7. Persoane împuternicite

Persoanele împuternicite implicate în prelucrări au următoarele responsabilități:

- a) respectă toate politicile privind confidențialitatea și protecția datelor aplicabile pentru prelucrările de date cu caracter personal efectuate,
- b) sunt responsabile pentru menținerea protecției și confidențialității tuturor informațiilor încredințate,
- c) informează Șefii entităților organizatorice despre încălcările reale sau presupuse ale politicilor de confidențialitate a datelor din zona lor de responsabilitate (incidente privind confidențialitatea datelor).

INFORMARE PRIVIND CONFIDENȚIALITATEA DATELOR CU CARACTER PERSONAL (SUPRAVEGHERE VIDEO)

Conform Regulamentului UE 679/2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, **Incarmed SRL** este un operator de date. Datele de contact sunt următoarele: **Calimanesti. Calea lui Traian nr. 734.**

CUM COLECTĂM / PRELUCRĂM INFORMAȚII DESPRE DUMNEAVOASTRĂ

INCARMED SRL, prin intermediul sistemelor de supraveghere video, colectează și prelucrează înregistrări video în scopul asigurării securității persoanelor și bunurilor, pazei și protecției bunurilor, imobilelor, valorilor și a materialelor utilizate în furnizarea serviciilor medicale precum și pentru prevenirea și combaterea infracționalității.

Spitalul utilizează un sistem de supraveghere video 24 ore/zi, 7 zile/săptămână pentru a preveni, descuraja, gestiona și ancheta incidentele de siguranță și securitate, precum și pentru protecția persoanelor și bunurilor împotriva incendiilor, furturilor, distrugerilor, atacurilor sau a oricăror amenințări.

Sistemul de supraveghere video ajută la prevenirea, descurajarea, gestionarea și, dacă este necesar, anchetarea incidentelor legate de siguranță și securitate, a potențialelor amenințări sau a accesului fizic neautorizat, inclusiv a accesului neautorizat în clădirile securizate și în sălile protejate, la infrastructura IT sau la aparatura existentă. Sistemul nu este utilizat pentru a monitoriza prezența angajaților.

Utilizarea sistemului de supraveghere video este menționată pe pictogramele poziționate la o distanță rezonabilă de locurile unde sunt amplasate echipamentele de supraveghere video, așa cum este prevăzut de GDPR, de Legea nr. 333/ 2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor precum și de Hotărârea Guvernului nr. 301/ 2012 pentru aprobarea Normelor metodologice de aplicare a Legii nr. 333 /2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor.

În afara sistemelor de supraveghere video amplasate conform cerințelor Legii nr. 333/ 2003, în anumite zone sunt instalate sisteme de supraveghere video în baza interesului legitim urmărit de către organizație. Utilizarea acestor sisteme de supraveghere este menționată pe pictogramele poziționate la o distanță rezonabilă de locurile unde sunt amplasate echipamentele de supraveghere video.

Supravegherea prin mijloace video se utilizează doar în situația în care mijloacele convenționale aplicate sunt considerabil mai puțin eficiente în realizarea obiectivelor menționate, conform analizei de risc efectuate la nivelul organizației.

Incarmed SRL nu prelucrează în scop privat datele cu caracter personal rezultate în urma monitorizării video iar sistemul de supraveghere nu este utilizat pentru monitorizarea activității angajaților sau colaboratorilor sau pentru pontajul angajaților.

Sistemul video existent a fost instalat în urma unor analize de risc, anexate planurilor de protecție și pază. Zonele supravegheate video cuprind:

- zone de acces și spații destinate publicului,
- zone cu acces restricționat
- împrejurimile clădirilor pentru a proteja spațiile exterioare

Nu sunt monitorizate zone în care există un nivel ridicat al așteptărilor privind viața privată, precum birouri, toalete sau alte locații similare.

TEMEIUL JURIDIC AL PRELUCRĂRILOR DE DATE CU CARACTER PERSONAL

Informațiile sunt prelucrate în mod legal în conformitate cu:

Legea nr. 95/2006 privind reforma în domeniul sănătății;

Legea nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor și normele de aplicare ale acesteia;

Hotărârea nr. 301 din 11 aprilie 2012 pentru aprobarea Normelor Metodologice a Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor;

Regulamentul UE 679/2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal;

Legea 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;

Decizia nr.174/2018 a Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal – ANSPDCP privind lista operațiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecției datelor cu caracter personal.

Din punct de vedere al Regulamentului UE 679/2016, supravegherea video se desfășoară în temeiul art.6(1) c – prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului sau în temeiul art. 6(1) d – prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice.

CATEGORIILE DE DESTINATARI AI DATELOR CU CARACTER PERSONAL

În măsura permisă de legislația privind protecția datelor, pentru a ne îndeplini obligațiile contractuale și legale putem transmite sau permite accesul la imaginile înregistrate unor autorități naționale.

CUM PROTEJĂM INFORMAȚIILE CONFIDENȚIALE COLECTATE

Informațiile colectate sunt păstrate în formă electronică iar pentru protecția acestora sunt implementate următoarele măsuri tehnice și organizatorice:

- limitarea timpului de stocare a imaginilor conform cerințelor legale;
- control acces înregistrări. Doar administratorul de sistem (desemnat de oreganizatie), are dreptul de a acorda, modifica sau anula dreptul de acces al utilizatorilor;
- instruire privind cerințele legate de confidențialitatea datelor și acorduri de confidențialitate pentru persoanele (angajați ai organizației sau ai persoanelor împuternicite) care vizualizeaza imaginile care se derulează în timp real sau au acces la imaginile înregistrate;
- asigurarea contractuală sau prin acorduri că persoane împuternicite folosite implementează măsuri tehnice și organizatorice de protecție a datelor.

LOCAȚIA DE STOCARE ȘI DURATA DE STOCARE

Datele cu caracter personal colectate sunt stocate pe echipamente situate în cadrul organizației. Durata de stocare este în conformitate cu cerințele legale (**30 de zile**), după acest interval imaginile ștergându-se automat în ordinea în care au fost înregistrate.

DREPTURI LEGATE DE PRELUCRAREA DATELOR CU CARACTER PERSONAL

Conform Regulamentului UE 679/2016, aveți următoarele drepturi:

- dreptul la informare. Aveți dreptul să primiți informații despre cum și de ce prelucrăm datele dumneavoastră personale;
- dreptul de a obține din partea organizației o confirmare că se prelucrează sau nu date cu caracter personal care vă privesc și, în caz afirmativ, acces la datele respective;
- dreptul de rectificare a datelor cu caracter personal care vă privesc;
- dreptul de ștergere a datelor cu caracter personal care vă privesc sau de restricționare a prelucrării, sub rezerva anumitor excepții;
- dreptul de a vă opune prelucrărilor, sub rezerva anumitor excepții.

Dacă doriți să faceți o solicitare în temeiul Regulamentului UE 679/2016, pentru a putea să vă răspundem într-un mod eficient va trebui să ne furnizați identitatea dumneavoastră (nume complet, date identificare) și indicații privind informațiile pe care le solicitați.

În cazul solicitării de acces la imagini înregistrate care vă privesc, soluționarea cererii se poate face prin acordarea accesului la înregistrarea solicitată sau prin transmiterea unei copii a acesteia. Cererea de acces trebuie să menționeze data, ora, locația pentru care se dorește acces la înregistrarea camerei de supraveghere.

Înregistrarea furnizată în cazul solicitării de acces depinde de condițiile tehnice de înregistrare, de condițiile în care a avut loc preluarea imaginilor și de drepturile altor persoane care pot apărea în înregistrare (imaginile în care apar alte persoane vor fi editate astfel încât să nu fie posibilă recunoașterea/identificarea lor). Este posibilă

restricționarea accesului pentru protejarea drepturilor și libertăților altor persoane (de exemplu dacă în imagini apar și alte persoane și nu există posibilitatea de a obține consimțământul lor sau imaginile acestora nu se pot edita).

Dacă aveți nemulțumiri legate de modul în care prelucrăm datele dumneavoastră cu caracter personal, aveți dreptul de a depune o plângere în fața Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, www.dataprotection.ro.

MODIFICĂRI ALE INFORMĂRII PRIVIND CONFIDENȚIALITATEA DATELOR

Având în vedere posibilitatea identificării unor noi prelucrări de date de natură personală, faptul că legile privind protecția datelor cu caracter personal și recomandările autorității de supraveghere se schimbă și se îmbunătățesc periodic, este posibil ca această informare privind confidențialitatea datelor să se schimbe și ea. Ne rezervăm dreptul de a modifica în orice moment, din orice motiv și fără notificare acest document de informare. Orice modificare a informării privind confidențialitatea va fi disponibilă pentru consultare la aviziere și afișată pe site-ul societății.

ÎNTREBĂRI, NELĂMURIRI, RECLAMAȚII

Dacă aveți întrebări cu privire la datele dumneavoastră personale, dacă doriți să vă exercitați drepturile sau aveți nelămuriri sau reclamații legate de modul în care gestionăm datele cu caracter personal, vă rugăm să contactați Responsabilul de Protecția Datelor la adresa de email dpo@sicc.ro.

Formular evidență modificări

Nr. crt.	Ediția	Data ediției	Revizia	Data reviziei	Nr. pag.	Descriere modificare	Semnătura conducătorului compartimentului
1	2	4	5	6	7	8	9
1	I	03.09.2018	-	-	12	- Elaborare conform OSGG 600/2018	