



MINISTERUL SĂNĂTĂȚII AL REPUBLICII MOLDOVA

ORDIN

mun. Chișinău

„28” august 2026

Nr. 677

Cu privire la aprobarea Ghidului privind protecția datelor cu caracter personal în domeniul sănătății

În temeiul pct. 2 al Programului național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025–2029, aprobat prin Hotărârea Guvernului nr. 306/2025, art. 89 alin. 2 lit. b) a Legii nr. 195/2024 privind protecția datelor cu caracter personal în activitatea instituțiilor din domeniul sănătății,

ORDON:

1. Se aprobă:
 - 1.1. Ghidul privind protecția datelor cu caracter personal în domeniul sănătății (în continuare - Ghid), conform anexei nr. 1;
 - 1.2. Formularele și materialele de afișare la Ghid, conform anexei nr. 2.
2. Conducătorii instituțiilor din domeniul sănătății vor aduce Ghidul la cunoștința personalului și vor asigura respectarea obligațiilor prevăzute de cadrul normativ aplicabil, utilizând și adaptând, după caz, recomandările, formularele-model și materialele prevăzute în anexa nr. 2.
3. Direcția juridică va asigura revizuirea Ghidului ori de câte ori intervin modificări ale cadrului normativ în domeniul protecției datelor cu caracter personal.
4. Se abrogă Ordinul nr. 791/2019 cu privire la unele măsuri pentru înregistrarea Ministerului și a prestatorilor de servicii medicale în calitate de operatori de date cu caracter personal, inclusiv a sistemelor de evidență a datelor cu caracter personal gestionate de către aceasta.
5. Controlul asupra executării prezentului ordin mi-l asum.

Ministru

Alexandru GASNAȘ

Anexa nr. 1
la Ordinul ministrului sănătății nr. 677 din 28 august 2026



MINISTERUL SĂNĂTĂȚII AL REPUBLICII MOLDOVA

GHID

privind protecția datelor cu caracter personal în domeniul sănătății

Chișinău, 2026

Aprobat prin Ordinul ministrului sănătății nr. 415 din 26 mai 2026
cu privire la aprobarea Ghidului privind protecția datelor cu caracter personal în domeniul sănătății

CUPRINS

Generalități	5
Abrevierile utilizate	5
Lista figurilor	6
Grupul de lucru	6
Prefața	6
Utilizatorii ghidului	7
Scopul ghidului	7
Obiectivele ghidului	7
Cadrul normativ de referință	7
CAPITOLUL I. NOȚIUNI ȘI PRINCIPII FUNDAMENTALE	9
1.1. Categoriile de date cu caracter personal	9
1.2. Categoriile speciale de date	9
1.3. Principiile prelucrării datelor	10
1.4. Temeiul juridic al prelucrării	12
1.5. Consimțământul — condiție, nu temei universal	12
CAPITOLUL II. GUVERNANȚA ȘI RESPONSABILITĂȚILE INSTITUȚIONALE	13
2.1. Guvernanța datelor în instituția medicală	13
2.2. Rolul conducerii instituției	13
2.3. Responsabilul cu protecția datelor	14
2.4. Registrul evidențelor activităților de prelucrare	14
2.5. Evaluarea impactului asupra protecției datelor	14
2.6. Relația cu persoanele împuternicite	15
CAPITOLUL III. DREPTURILE PACIENTULUI	16
3.1. Drepturile persoanei vizate	16
3.2. Procedura de soluționare a cererilor	16
3.3. Accesul terților și al aparținătorilor	17
CAPITOLUL IV. CONDUITA PROFESIONALĂ ȘI SECURITATEA PRELUCRĂRII	18
4.1. Conduita profesională a personalului	18
4.2. Canale de comunicare permise	18
4.3. Măsuri de securitate	18
4.4. Sistemele informaționale și controlul accesului	19
4.5. Accesul personalului tehnic	19
4.6. Confidențialitatea în spațiul fizic și pe suport de hârtie	20

4.7.	Videosupravegherea	21
CAPITOLUL V. REGIMURI ȘI SITUAȚII SPECIFICE		22
5.1.	Regimuri speciale de confidențialitate	22
5.2.	Cercetarea în domeniul sănătății	22
5.3.	Transmiterea datelor și transferurile în afara țării	23
5.4.	Solicitările autorităților și ale terților	23
5.5.	Datele cu caracter personal ale personalului	23
CAPITOLUL VI. INCIDENTELE DE SECURITATE ȘI RĂSPUNDEREA		25
6.1.	Gestionarea incidentelor de securitate	25
6.2.	Consecințele neconformității	25
CAPITOLUL VII. INSTRUMENTE DE APLICARE		27
7.1.	Situații practice	27
7.2.	Întrebări frecvente	29
7.3.	Autoevaluarea conformității	30
7.4.	Aplicarea și actualizarea ghidului	30
Glosar		31
Formulare și materiale de afișare		31

GENERALITĂȚI

Abrevierile utilizate

AMP	Asistența medicală primară
AMS	Asistența medicală spitalicească
ANSP	Agenția Națională pentru Sănătate Publică
CNAM	Compania Națională de Asigurări în Medicină
CNAS	Casa Națională de Asigurări Sociale
CNEAS	Consiliul Național de Evaluare și Acreditare în Sănătate
CNPDCP	Centrul Național pentru Protecția Datelor cu Caracter Personal
DES	Dosarul electronic de sănătate
eRețeta	Sistemul informațional pentru prescripția electronică a medicamentelor compensate
GDPR	Regulamentul (UE) 2016/679 privind protecția datelor cu caracter personal
IDNP	Numărul de identificare de stat al persoanei fizice
IMSP	Instituție medico-sanitară publică
MS	Ministerul Sănătății
PCCM	Portalul certificatelor de concediu medical (esanatate.gov.md)
RPD	Responsabilul cu protecția datelor cu caracter personal
SIA	Sistem informațional automatizat
SM ISO/IEC	Standard moldovenesc care preia un standard internațional

EIPD	Evaluarea impactului asupra protecției datelor
------	--

Lista figurilor

Figura 1	Clasificarea datelor în sistemul de sănătate, în funcție de sensibilitate
Figura 2	Principiile prelucrării datelor cu caracter personal
Figura 3	Modelul de guvernanță a datelor în instituția medicală
Figura 4	Repartizarea responsabilităților între structurile instituției
Figura 5	Drepturile persoanei vizate
Figura 6	Arbore decizional pentru solicitările de acces la documentația medicală
Figura 7	Controlul accesului și trasabilitatea în sistemele informaționale

Grupul de lucru

Ghidul a fost elaborat de grupul de lucru instituit la nivelul Ministerului Sănătății prin Ordinul ministrului sănătății nr. 415 din 26 mai 2026.

Prefața

Confidențialitatea informației privind pacientul este o componentă a actului medical de calitate, alături de competența profesională și de consimțământul informat. Datele privind sănătatea se numără printre cele mai sensibile categorii de date cu caracter personal, iar divulgarea sau utilizarea lor necorespunzătoare afectează demnitatea, statutul profesional și siguranța persoanei.

Ghidul transpune obligațiile legale privind protecția datelor în repere de conduită profesională aplicabile în activitatea curentă a instituțiilor din domeniul sănătății. El a fost elaborat în contextul aplicării, de la 23 august 2026, a Legii nr. 195/2024 privind protecția datelor cu caracter personal, care înlocuiește Legea nr. 133/2011 și aliniază cadrul național la standardele europene în materie.

Ghidul realizează acțiunea nr. 61 din anexa B la capitolul 28 „Protecția consumatorilor și a sănătății” al Programului național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025–2029, aprobat prin Hotărârea Guvernului nr. 306/2025, și susține obiectivele Programului național pentru digitalizare și inovare în sănătate pe anii 2025–2030, aprobat prin Hotărârea Guvernului nr. 556/2025, în componenta de securitate și guvernanță a datelor.

Statutul documentului

Ghidul are caracter de recomandare. Nu instituie obligații suplimentare față de cadrul normativ și nu se substituie acestuia. În caz de neconcordanță prevalează dispozițiile legale. Recomandările se aplică ținând seama de specificul fiecărei instituții și de evaluarea proprie a riscurilor.

Utilizatorii ghidului

- prestatorii publici și privați de servicii medicale și farmaceutice — personalul medical, administrativ și tehnic implicat în prelucrarea datelor;
- instituțiile, agențiile și autoritățile din sistemul de sănătate;
- organizațiile necomerciale autorizate să presteze servicii medicale;
- instituțiile de învățământ medical — personalul didactic, studenții și rezidenții, în măsura accesului la informația medicală.

Scopul ghidului

Stabilirea unui cadru unitar de bune practici pentru prelucrarea datelor cu caracter personal în domeniul sănătății, în conformitate cu cadrul normativ al Republicii Moldova.

Obiectivele ghidului

- aplicarea unitară a legislației privind protecția datelor în activitatea medico-sanitară;
- repere practice pentru colectarea, utilizarea, transmiterea, păstrarea și arhivarea datelor pacienților;
- clarificarea drepturilor pacienților și a modului concret de exercitare a acestora;
- consolidarea măsurilor tehnice și organizatorice de securitate a informației medicale.

Cadrul normativ de referință

Prelucrarea datelor cu caracter personal în domeniul sănătății se realizează cu respectarea, în principal, a următoarelor acte normative ale Republicii Moldova:

Act normativ	Obiectul reglementării
Legea nr. 195/2024 privind protecția datelor cu caracter personal	Cadrul general, aplicabil de la 23 august 2026. Înlocuiește Legea nr. 133/2011, care rămâne aplicabilă prelucrărilor și faptelor anterioare acestei date.
Legea ocrotirii sănătății nr. 411/1995	Secretul medical și obligațiile lucrătorului medical.
Legea nr. 263/2005 cu privire la drepturile și responsabilitățile pacientului	Confidențialitatea informațiilor ce constituie secret medical și condițiile de acces la documentația medicală.
Legea nr. 264/2005 cu privire la exercitarea profesiei de medic	Obligațiile profesionale ale medicului.
Legea nr. 23/2007 cu privire la profilaxia infecției HIV/SIDA; Legea nr. 1402/1997 privind sănătatea mentală; Legea nr. 153/2008 cu privire la controlul și profilaxia tuberculozei	Regimuri speciale de confidențialitate.
Legea nr. 48/2023 privind securitatea cibernetică; Hotărârea Guvernului nr. 201/2017	Cerințele minime obligatorii de securitate cibernetică aplicabile sistemelor informaționale.
Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate	Schimbul de date între sistemele și registrele naționale (platforma MConnect).
Legea nr. 91/2014 privind semnătura electronică și documentul electronic	Valoarea juridică a documentelor medicale electronice.
Legea nr. 880/1992 privind Fondul Arhivistic al Republicii Moldova	Termenele de păstrare și nomenclatorul dosarelor.
Hotărârea Guvernului nr. 192/2017	Codul deontologic al lucrătorului medical și al farmacistului.
Hotărârea Guvernului nr. 306/2025 — Programul național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025–2029	Anexa B la capitolul 28 „Protecția consumatorilor și a sănătății”, acțiunea nr. 61 — elaborarea ghidului privind asigurarea datelor cu caracter personal în domeniul medical (termen: august 2026; responsabili: Ministerul Sănătății și CNPDCP).
Hotărârea Guvernului nr. 556/2025 — Programul național pentru digitalizare și inovare în sănătate pe anii 2025–2030	Dezvoltarea sistemelor informaționale din sănătate, inclusiv a dosarului electronic de sănătate, cu consolidarea securității și a guvernantei datelor.

Ca repere de bună practică se utilizează standardele RM care preiau standardele internaționale în domeniul securității informației — SM ISO/IEC 27001 și SM ISO/IEC 27799 — precum și, cu titlu de referință pentru armonizarea cadrului național, Regulamentul (UE) 2016/679 și orientările Centrului Național pentru Protecția Datelor cu Caracter Personal.

CAPITOLUL I. NOȚIUNI ȘI PRINCIPII FUNDAMENTALE

1.1. Categoriile de date cu caracter personal

Datele cu caracter personal reprezintă orice informație prin care o persoană fizică poate fi identificată, direct sau indirect. Identificarea poate rezulta dintr-un singur element — nume, IDNP — sau dintr-o combinație de detalii care, împreună, indică o anumită persoană.

Categorie	Exemple în activitatea medicală	Nivel de protecție
Date de identificare	Nume, prenume, IDNP, buletin de identitate	De bază
Date de contact	Adresă, telefon, e-mail	De bază
Date privind sănătatea	Diagnostic, tratament, investigații, documentație medicală	Special
Date genetice	Profil ADN, analize cromozomiale	Special
Date biometrice	Amprentă, recunoaștere facială pentru controlul accesului	Special
Viața sexuală și reproductivă	Istoric reproductiv, planificare familială	Special
Date socio-administrative	Stare civilă, statutul de persoană asigurată	De bază
Date financiare	Conturi pentru decontări, venituri	Restricționat

Identificarea indirectă

Eliminarea numelui nu echivalează cu anonimizarea. O persoană poate fi identificată și prin context — de exemplu, prin asocierea secției, a datei intervenției și a medicului curant.

1.2. Categoriile speciale de date

Datele privind sănătatea, datele genetice și datele biometrice prelucrate în scopul identificării unice constituie categorii speciale de date. Regula este interdicția prelucrării lor, cu excepția situațiilor prevăzute expres de lege — acordarea asistenței medicale și gestionarea serviciilor de sănătate fiind temeiul principal în practica curentă.

Accesul rămâne limitat la personalul implicat în îngrijire și este condiționat de obligația păstrării secretului medical, aplicabilă întregului personal cu acces la informația medicală, inclusiv personalului tehnic. Figura 1 prezintă nivelurile de protecție corespunzătoare fiecărei categorii de date.

CLASIFICAREA DATELOR ÎN SISTEMUL DE SĂNĂTATE

Nivelul măsurilor de protecție corespunde gradului de sensibilitate

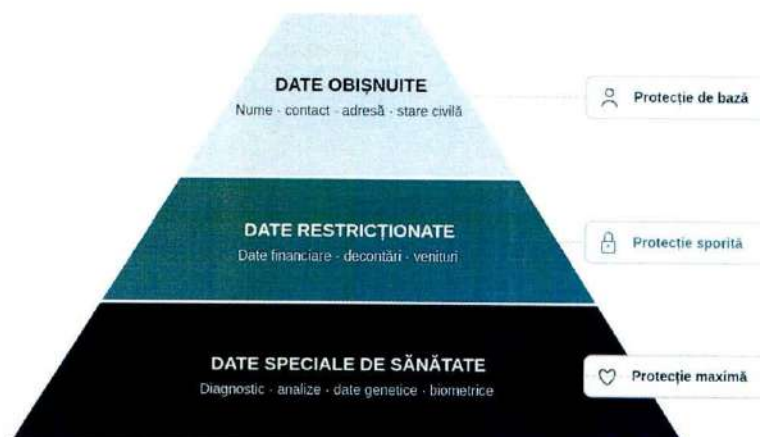


Figura 1. Clasificarea datelor în sistemul de sănătate, în funcție de sensibilitate.

Regula de bază

Orice informație care relevă starea de sănătate a unei persoane este tratată la cel mai înalt nivel de protecție. Confirmarea internării sau a prezenței unei persoane în instituție, către terți neautorizați, constituie deja o divulgare nepermisă.

1.3. Principiile prelucrării datelor

Întreaga reglementare se întemeiază pe șase principii de prelucrare, completate de principiul responsabilizării. Acestea se aplică oricărei operațiuni cu date de pacient și sunt sintetizate în Figura 2.

CELE 7 PRINCIPII DE PRELUCRARE A DATELOR

Fundamentul oricărei activități cu date de pacient



Figura 2. Principiile prelucrării datelor cu caracter personal.

Principiul	Ce înseamnă în activitatea medicală
Legalitate, echitate, transparență	Datele se prelucrează în temeiul unui motiv legal, iar pacientul este informat, anterior colectării, cu privire la operator, scopuri, destinatari și durata prelucrării.

Principiul	Ce înseamnă în activitatea medicală
Limitarea scopului	Datele colectate pentru îngrijire nu se utilizează în scopuri incompatibile fără un temei distinct. Prelucrarea ulterioară în scopuri de cercetare, statistică sau arhivare este compatibilă, cu garanțiile prevăzute de lege.
Reducerea la minimum	Se colectează exclusiv datele necesare scopului declarat. Formularele și câmpurile sistemelor informaționale se revizuiesc periodic.
Exactitatea	Verificarea identității la adresare și mecanismele de rectificare previn erori cu impact asupra siguranței pacientului.
Limitarea stocării	Datele se păstrează pe perioadele prevăzute de nomenclatorul dosarelor aprobat al instituției, după care se șterg sau se anonimizează.
Integritate și confidențialitate	Datele se protejează prin măsuri tehnice și organizatorice proporționale cu riscul.
Responsabilizare	Operatorul nu numai că respectă principiile, ci trebuie să poată demonstra respectarea lor: politici, registre, evaluări de risc, evidența instruirilor, jurnalizarea accesărilor.

1.3.1. Termenele de păstrare

Termenele nu se stabilesc de la caz la caz. Instituția aprobă un nomenclator al dosarelor, corelat cu Indicatorul documentelor-tip și cu indicatoarele de ramură, care fixează pentru fiecare categorie documentară termenul de păstrare, locul de păstrare și modalitatea de eliminare la expirare. Termenul din nomenclator prevalează asupra unei cereri de ștergere.

Categorie de documente	Termen propus*	Observație
Fișa medicală a bolnavului de staționar (F-003/e)	25 de ani de la externare	Se păstrează integral, inclusiv anexele clinice și consimțămintele.
Fișa medicală de ambulator (F-025/e)	25 de ani de la ultima adresare	La transferul pacientului se transmite instituției care preia îngrijirea.
Registre medicale (internări, gardă, intervenții)	25 de ani	Pe suport de hârtie: spațiu încuiat, evidență de predare-primire.
Rezultate de laborator și investigații imagistice	5–10 ani	Rezultatele anexate fișei urmează termenul fișei.
Consimțăminte, note de informare, cereri ale persoanelor vizate	Durata relației plus 3 ani	Element de demonstrare a conformității.
Contracte cu persoanele împuternicite	Durata contractului plus 3 ani	Inclusiv dovezile de ștergere la încetare.
Registrul incidentelor de securitate	5 ani	Se păstrează inclusiv incidentele nenotificate.
Jurnalele de acces în sistemele informaționale	Minimum 12 luni	Protejate împotriva modificării; 24 de luni recomandat.
Înregistrări video	Maximum 30 de zile	Prelungire numai pentru un incident documentat, până la soluționare.
Dosarul personal al angajatului	75 de ani	Acces restrâns, separat de fișa de medicina muncii.

* Termenele propuse se confirmă prin nomenclatorul dosarelor aprobat al instituției, coordonat cu Serviciul de Stat de Arhivă, înainte de aplicare.

1.4. Temeiul juridic al prelucrării

Prelucrarea datelor de sănătate se întemeiază, de regulă, pe necesitatea acordării asistenței medicale, pe îndeplinirea unei obligații legale a operatorului ori, în situații limitate, pe protejarea intereselor vitale ale pacientului sau pe interesul public în domeniul sănătății publice. Prelucrarea se realizează de personal supus obligației secretului medical sau sub răspunderea acestuia.

Situație curentă	Temeiul prelucrării	Ce NU este necesar
Consultație, diagnostic, tratament, îngrijire	Necesitatea acordării asistenței medicale	Consimțământul pentru prelucrarea datelor. Consimțământul informat pentru actul medical rămâne o cerință separată.
Raportări către CNAM, ANSP și alte autorități	Obligație legală a operatorului	Acordul pacientului.
Pacient în imposibilitate de a-și exprima voința	Protejarea intereselor vitale	Amânarea îngrijirii pentru obținerea unui acord formal.
Supraveghere epidemiologică	Interes public în domeniul sănătății publice	Acordul pacientului.
Fotografii clinice, prezentări de caz, publicare	Consimțământ explicit, distinct	—
Participarea la un studiu de cercetare	Consimțământ explicit, cu aviz etic	—

1.5. Consimțământul — condiție, nu temei universal

În activitatea medicală curentă consimțământul nu constituie temeiul prelucrării, ci o condiție suplimentară de legalitate, cerută doar pentru prelucrările enumerate mai sus. Atunci când prelucrarea se întemeiază pe consimțământ, acesta trebuie să fie liber, specific, informat și neechivoc și poate fi retras oricând, la fel de simplu cum a fost acordat.

Eroarea frecventă

Solicitarea consimțământului pentru o prelucrare care este oricum necesară îngrijirii sau impusă de lege creează pacientului așteptarea că poate refuza o prelucrare care, în realitate, nu poate fi oprită.

CAPITOLUL II. GUVERNANȚA ȘI RESPONSABILITĂȚILE INSTITUȚIONALE

2.1. Guvernanța datelor în instituția medicală

Guvernanța datelor reprezintă ansamblul de roluri, responsabilități, politici și procese prin care instituția asigură prelucrarea legală, sigură și coerentă a datelor. Ea stabilește cine răspunde de ce, cum circulă datele și cum se gestionează riscurile. Modelul este reprezentat în Figura 3.



Figura 3. Modelul de guvernanță a datelor în instituția medicală.

Trei întrebări de guvernanță

- Ce date prelucrăm și cât de sensibile sunt? (clasificare)
- Cine răspunde de fiecare activitate? (roluri și responsabilități)
- Ce riscuri există și cum le tratăm? (managementul riscurilor)

Fiecare categorie de date parcurge un ciclu de viață: colectare, utilizare, stocare, partajare, arhivare și ștergere sau anonimizare. Instituția documentează acest circuit în registrul evidențelor, identificând pentru fiecare activitate scopul, temeiul, destinatarii, termenele și măsurile de securitate.

2.2. Rolul conducerii instituției

Conducerea instituției medicale, în calitate de operator de date, poartă răspunderea pentru conformitate. Protecția datelor este o responsabilitate de management, nu exclusiv una tehnică sau a responsabilului cu protecția datelor.

- aprobă politicile și procedurile interne și asigură aplicarea lor;
- desemnează responsabilul cu protecția datelor și îi garantează independența funcțională;
- asigură resursele umane, financiare și tehnice necesare — subdimensionarea resurselor constituie, ea însăși, un factor de risc;
- instituie un program de instruire periodică, cel puțin anuală, cu evidența ținută potrivit formularului F-17, și se asigură că noii angajați sunt instruiți la încadrare și semnează angajamentul de confidențialitate (formularul F-08);
- dispune evaluări interne periodice și adoptă măsuri corective.

2.3. Responsabilul cu protecția datelor

Instituțiile care prelucrează date de sănătate la scară largă și autoritățile publice din domeniu desemnează un responsabil cu protecția datelor. Acesta informează și consiliază, monitorizează conformitatea, coordonează evaluările de impact, cooperează cu autoritatea de supraveghere și constituie punct de contact pentru persoanele vizate.

Responsabilul cu protecția datelor își exercită atribuțiile în mod independent, nu poate fi sancționat pentru îndeplinirea lor și raportează nivelului superior de conducere. Răspunderea pentru conformitate rămâne a operatorului. Instituțiile mici pot desemna un responsabil partajat, cu condiția ca acesta să fie accesibil personalului și pacienților.

Repartizarea orientativă a atribuțiilor între conducere, responsabilul cu protecția datelor, structura informatică și personalul medical este redată în Figura 4.

MATRICE DE RESPONSABILITĂȚI (RACI)
Repartizarea atribuțiilor privind protecția datelor pe roluri instituționale

Activitate	Conducere	DPO	IT / Securitate	Personal medical	Persoană împuternicită
Politici de protecție a datelor	A	C	C	I	I
Registrul evidențelor (art. 30)	A	R	C	I	I
Evaluarea de impact (DPIA)	A	R	C	C	C
Instruirea personalului	A	R	C	I	I
Controlul accesului în sisteme	A	C	R	I	I
Notificarea incidentelor	A	R	R	I	C
Soluționarea cererilor pacienților	A	R	C	C	I
Contracte cu împuterniciți (art. 28)	A	C	C	I	R

R Realizează A Răspunde C Consultat I Informat

Figura 4. Repartizarea responsabilităților între structurile instituției.

2.4. Registrul evidențelor activităților de prelucrare

Instituția menține un registru al activităților de prelucrare care cuprinde scopurile, categoriile de date și de persoane vizate, destinatarii, termenele de stocare și descrierea măsurilor de securitate. Derogarea aplicabilă entităților mici nu operează în domeniul medical, întrucât se prelucrează în mod curent date de sănătate.

Registrul se întocmește folosind formularul F-10, se actualizează la fiecare modificare de sistem sau de flux și se revizuieste integral anual. Este primul document solicitat în cazul unui control.

2.5. Evaluarea impactului asupra protecției datelor

Se efectuează o evaluare de impact anterior prelucrărilor susceptibile să genereze un risc ridicat, în special pentru:

- dosarul electronic de sănătate și interconectarea sistemelor informaționale naționale;
- soluțiile de inteligență artificială utilizate în diagnostic, prognostic sau triaj;
- prelucrarea la scară largă a datelor genetice sau biometrice;
- integrarea sistemelor de laborator și imagistică, telemedicina și serviciile de tip cloud;
- transferurile de date în afara țării în absența unor garanții adecvate.

Grila de determinare și structura raportului se află în formularul F-11. Atunci când riscul ridicat nu poate fi atenuat prin măsuri rezonabile, se consultă în prealabil autoritatea de supraveghere.

2.6. Relația cu persoanele împuternicite

Colaborarea cu laboratoare externe, furnizori de servicii informatice, servicii de tip cloud sau de arhivare se realizează în baza unui contract de prelucrare. Clauzele minime sunt prevăzute în formularul F-09.

- accesul furnizorului la mediul de producție se acordă punctual, pe interval limitat, cu cont nominal, autentificare cu mai mulți factori, aprobare prealabilă și înregistrarea sesiunii, cu revocarea drepturilor la închiderea solicitării;
- în achizițiile publice, cerințele de protecție a datelor se formulează ca cerințe de conformitate demonstrabilă, verificabile la recepție: control al accesului pe rol, pistă de audit, export de jurnale, pseudonimizare, interoperabilitate potrivit standardelor aplicabile;
- locația efectivă de stocare a datelor se verifică contractual, nu se presupune.

CAPITOLUL III. DREPTURILE PACIENTULUI

3.1. Drepturile persoanei vizate

Pacientul dispune de drepturile prevăzute de legislația aplicabilă asupra datelor sale. Cererile se soluționează gratuit și fără întârziere nejustificată, în termen de o lună, cu posibilitatea unei prelungiri justificate în cazuri complexe. Drepturile sunt sintetizate în Figura 5.



Figura 5. Drepturile persoanei vizate.

Drept	Conduita instituției	Particularități în domeniul medical
Informare	Furnizarea notei de informare la colectare (formularul F-01)	Comunicarea unui diagnostic sever poate fi mediată de medicul curant.
Acces	Eliberarea unei copii, după verificarea identității	Fără afectarea drepturilor terților.
Rectificare	Corectarea datelor inexacte; completarea cu o declarație	Aprecierile clinice se mențin; pot fi completate.
Ștergere	Evaluare împreună cu responsabilul cu protecția datelor	Limitat: prevalează arhivarea legală și interesul de sănătate publică.
Restricționare	Suspendarea utilizării active, cu păstrarea datelor	Stocarea continuă.
Portabilitate	Furnizarea datelor într-un format structurat	Numai datele furnizate de persoană, prin mijloace automate.
Opoziție	Analiză de la caz la caz	Nu se aplică îngrijirilor și raportărilor obligatorii.
Decizii automate	Asigurarea unei intervenții umane	Triajul și scorurile automate sunt supuse revizuirii umane.

3.2. Procedura de soluționare a cererilor

1	Cererea se depune în scris, pe suport de hârtie sau în format electronic, la registratură ori la responsabilul cu protecția datelor (formularul F-04).
2	Se verifică identitatea solicitantului — etapă obligatorie pentru datele medicale.
3	Cererea se înregistrează, cu dată și număr, în registrul cererilor persoanelor vizate (formularul F-06).
4	Se analizează cererea și se pregătește răspunsul, cu avizul responsabilului cu protecția datelor.

5	Răspunsul se comunică în termen de o lună; în cazuri complexe termenul poate fi prelungit, cu informarea prealabilă a solicitantului.
6	Eventualul refuz se motivează în scris, cu indicarea dreptului de a sesiza CNPDCP (formularul F-05).

3.3. Accesul terților și al aparținătorilor

Datele medicale ale unui pacient adult și capabil nu se comunică unei rude sau altui terț în absența acordului pacientului, a unei procuri ori a unui temei expres prevăzut de lege. Reprezentantul legal al unei persoane lipsite de capacitate accesează datele pe baza documentelor care atestă această calitate. Fiecare eliberare se consemnează folosind formularul F-07. Arborele decizional este prezentat în Figura 6.



* Excepție: reprezentantul legal al unei persoane incapacitate, cu documente justificative.

Figura 6. Arbore decizional pentru solicitările de acces la documentația medicală.

Precizare privind pacientul decedat. Decesul pacientului nu înlătură confidențialitatea datelor sale medicale: secretul medical și legislația națională aplicabilă continuă să le protejeze. Condițiile de accesare a documentației medicale de către rude se mențin aceleași — simpla legătură de rudenie nu conferă, prin ea însăși, dreptul de acces. Documentația se eliberează succesorului care prezintă certificatul de deces și dovada calității sau persoanei care invocă un temei expres prevăzut de lege, după verificarea identității solicitantului. Eliberarea se consemnează în formularul F-07.

CAPITOLUL IV. CONDUITA PROFESIONALĂ ȘI SECURITATEA PRELUCRĂRII

4.1. Conduita profesională a personalului

Principiul fundamental: datele unui pacient se accesează și se prelucrează exclusiv în scopul îngrijirii sau al unei atribuții legale, în limita strictă a necesității, și se protejează pe tot parcursul utilizării lor.

Acțiuni permise	Acțiuni nepermise
Accesarea documentației unui pacient aflat în îngrijirea proprie	Consultarea documentației din curiozitate — rude, colegi, persoane cunoscute
Utilizarea datelor pentru diagnostic și tratament	Confirmarea sau discutarea stării unui pacient cu persoane neautorizate
Transmiterea datelor către alt profesionist implicat în îngrijire, pe canale securizate	Transmiterea datelor prin canale necontrolate sau pe echipamente personale
Efectuarea raportărilor prevăzute de lege către autoritățile competente	Fotografierea pacienților sau a documentelor cu dispozitive personale
Prelucrarea în situații de urgență, pentru protejarea vieții	Utilizarea datelor în scopuri personale, comerciale sau de cercetare neaprobată

Cel mai frecvent tip de abatere

Accesarea nejustificată a documentației unei persoane cunoscute, în absența implicării în îngrijire, constituie abatere chiar și fără transmiterea ulterioară a informației. Fiecare accesare este înregistrată, poate fi auditată și este vizibilă pacientului în istoricul accesului.

4.2. Canale de comunicare permise

Transmiterea rezultatelor, imaginilor, listelor de pacienți sau a planurilor de tratament prin aplicații publice de mesagerie ori prin conturi personale de poșta electronică duce la pierderea controlului asupra datelor: dispare trasabilitatea, auditul devine imposibil, iar un mesaj expediat greșit nu mai poate fi retras. Comunicarea profesională se realizează exclusiv prin canalele instituționale.

- sistemul informațional al instituției trebuie să includă mesagerie internă securizată, partajare controlată de fișiere și consult interclinic legat de documentația pacientului;
- sistemul blochează exporturile nejustificate și înregistrează fiecare transmitere, descărcare, imprimare sau consultare externă;
- politica instituțională prevede toleranță zero pentru folosirea conturilor personale în prelucrarea datelor medicale.

4.3. Măsurile de securitate

Securitatea se asigură prin măsuri tehnice și organizatorice adecvate riscului, în corespundere cu cerințele minime obligatorii de securitate cibernetică și cu sensibilitatea datelor medicale.

Domeniu	Conținut	Prioritate
Autentificare	Doar MPass sau Parole robuste și autentificare cu mai mulți factori, cu ulterioara trecere la autentificare prin MPass	Esențială
Criptare	Criptarea datelor în tranzit și la stocare	Esențială
Control al accesului	Drepturi alocate pe rol; principiul necesității de a cunoaște	Esențială

Domeniu	Conținut	Prioritate
Copii de rezervă	Realizate periodic și testate prin restaurare	Ridicăta
Jurnalizare	Înregistrarea accesărilor: autor, moment, operațiune	Ridicăta
Echipamente mobile	Criptare și posibilitatea ștergerii la distanță	Medie

La nivel de conduită individuală: nedivulgarea datelor de acces și utilizarea exclusivă a contului propriu; blocarea sesiunii la fiecare părăsire a postului; politica „birou ordonat”; distrugerea securizată a documentelor pe suport de hârtie; participarea la instruirile periodice.

4.4. Sistemele informaționale și controlul accesului

Accesul în sistemele informaționale medicale este individual, alocat pe rol și jurnalizat. Lanțul de măsuri — identificare, autentificare, autorizare, acces minim, jurnalizare și audit — asigură că fiecare accesare este legitimă și verificabilă. Lanțul este ilustrat în Figura 7.



Figura 7. Controlul accesului și trasabilitatea în sistemele informaționale.

- accesul la modulele clinice se corelează cu programul de lucru, tura, garda sau implicarea documentată în episodul de îngrijire;
- accesul din afara instituției se permite numai prin rețea privată virtuală aprobată, cu autentificare multiplă și de pe echipamente gestionate de instituție;
- orice abatere de la contextul normal devine eveniment auditat: acces în afara turei, acces la un pacient fără relație clinică, export voluminos, căutări repetitive.

Drepturile se acordă pe rol, nu pe persoană. Matricea de acces pe roluri (formularul F-14) stă la baza configurării drepturilor în sistemele informaționale și se revizuieste semestrial.

Utilizarea sistemelor informaționale naționale nu transferă răspunderea instituției. Instituția răspunde pentru conturile pe care le administrează, pentru drepturile de acces acordate propriului personal și pentru legitimitatea fiecărei accesări efectuate de angajații săi, inclusiv atunci când datele sunt găzduite central. Cererile pacienților privind datele dintr-un sistem național se adresează instituției care a introdus datele.

4.5. Accesul personalului tehnic

Personalul tehnic și administratorii de sistem dispun, prin natura atribuțiilor, de acces privilegiat la infrastructură și, potențial, la date de sănătate.

- accesul privilegiat se acordă strict pentru sarcini de administrare și mentenanță, pe durata necesară, în temeiul unei autorizări documentate;

- conturile administrative sunt nominale și separate de conturile de utilizator curent;
- operațiunile efectuate cu drepturi privilegiate se jurnalizează, iar jurnalele se protejează împotriva modificării;
- obligația păstrării secretului medical se extinde asupra personalului tehnic; accesul tehnic nu autorizează consultarea conținutului clinic;
- atribuțiile critice se separă, astfel încât o singură persoană să nu poată, fără control, atât să acceseze date, cât și să modifice jurnalele de acces.

Bună practică

Drepturile de acces se revizuiesc periodic și se revocă în aceeași zi la încetarea raporturilor de muncă sau la schimbarea atribuțiilor. Conturile inactive se dezactivează.

4.6. Confidențialitatea în spațiul fizic și pe suport de hârtie

Cele mai frecvente divulgări nu se produc prin atacuri informatice, ci în activitatea obișnuită: un nume rostit cu voce tare, un monitor orientat spre sala de așteptare, o fișă lăsată pe ghișeu. Măsurile din prezentul punct nu presupun investiții și se aplică din prima zi.

Zonă	Reguli
Spațiile de primire și sălile de așteptare	Apelarea pacientului prin nume și prenume sau prin număr de ordine, fără menționarea motivului prezentării sau a diagnosticului. Monitoare se orientează astfel încât să nu fie vizibile din sala de așteptare. Se marchează o linie de discreție la ghișeu. Nu se afișează liste nominale.
Saloanele și vizita medicală	Panourile din saloane pot conține numele pacientului și date organizatorice, nu diagnosticul. Informațiile sensibile se comunică într-un spațiu separat. Prezența unui pacient nu se confirmă vizitatorilor neindicați de acesta.
Discuțiile profesionale	Dacă poate auzi o persoană neimplicată în îngrijire, discuția nu are loc. Sunt excluse discuțiile despre cazuri în lift, pe holuri, în cantină sau în transport. Obligația se menține și după încetarea raporturilor de muncă.
Documentația pe suport de hârtie	Păstrare în dulapuri sau încăperi încuiate, cu acces nominal. Predarea-primirea se consemnează în scris. La părăsirea postului documentele se pun în sertar; nu se lasă pe imprimantă sau copiator. Distrugerea se face securizat, prin tocare, pe bază de proces-verbal (formularul F-19).

Situație frecventă	Conduita corectă
Strigarea diagnosticului în sala de așteptare	Se apelează numele sau numărul de ordine, cu indicarea cabinetului.
Monitorul de la recepție vizibil pacienților	Reorientarea ecranului, filtru de confidențialitate, blocare automată.
Fișa lăsată pe ghișeu între doi pacienți	Fișa se închide și se pune în sertar înainte de apelarea următorului pacient.
Rezultate tipărite lăsate pe imprimanta comună	Tipărire cu eliberare la card sau cod; ridicare imediată.
Confirmarea internării către un apelant necunoscut	Nu se confirmă și nu se infirmă; se aplică procedura de la pct. 5.4.

4.7. Videosupravegherea

Videosupravegherea este o prelucrare de date cu caracter personal și, în context medical, poate genera date privind sănătatea. Se instalează numai pe baza unei decizii documentate a conducerii, cu scop determinat și cu avizul responsabilului cu protecția datelor (formularul F-18).

Zone în care este, de regulă, admisă	Zone în care este interzisă
Intrări, holuri de acces, scări, ascensoare	Saloane și rezerve
Zona de recepție a camerei de gardă	Cabinete de consultație, tratament și recoltare
Depozitul de medicamente	Săli de operație și de naștere, cu excepția unei justificări clinice documentate
Casierie, arhivă, camera serverelor	Vestiare, grupuri sanitare
Parcare și perimetru exterior	Spații de odihnă și de servire a mesei pentru personal

- informarea se realizează pe două niveluri: pictogramă vizibilă înaintea intrării în zonă și nota de informare completă, disponibilă la recepție;
- accesul la înregistrări se acordă nominal, prin decizie scrisă, iar fiecare vizionare se consemnează în registru;
- termenul de păstrare este aproximativ 30 de zile, cu prelungire numai pentru un incident documentat;
- camerele ascunse, înregistrarea audio și recunoașterea facială necesită un temei distinct și o evaluare de impact prealabilă;
- videosupravegherea nu se utilizează pentru monitorizarea activității sau a performanței personalului.

CAPITOLUL V. REGIMURI ȘI SITUAȚII SPECIFICE

5.1. Regimuri speciale de confidențialitate

Anumite categorii de informații medicale expun pacientul unui risc de stigmatizare, de discriminare sau de violență mult superior mediei. Pentru acestea, măsurile obișnuite se aplică într-o formă întărită, iar accesul se restrânge la personalul direct implicat în îngrijire.

Categorie	Măsuri specifice
Infecția HIV/SIDA și infecțiile cu transmitere sexuală	Acces nominal restrâns; rezultatele se comunică exclusiv direct pacientului; nu se menționează diagnosticul pe documente care circulă — bonuri, plicuri, etichete, certificate.
Tuberculoza și alte boli transmisibile	Raportările epidemiologice se transmit exclusiv în formatul și către destinatarii prevăzuți de normă; nu se comunică angajatorului sau comunității.
Sănătatea mintală și tulburările de consum de substanțe	Marcaj de sensibilitate în sistemul informațional; atenție sporită la solicitările aparținătorilor, care nu au drept de acces în absența acordului sau a calității de reprezentant legal.
Sănătatea reproductivă și întreruperea sarcinii	Confidențialitate întărită față de familie și partener; comunicarea se face exclusiv pacientei.
Victime ale violenței în familie sau ale infracțiunilor sexuale	Restricționarea vizibilității datelor de contact și de domiciliu; interdicția confirmării prezenței în instituție.
Date genetice, donare și transplant	Acces strict pe necesitate; pseudonimizare în utilizările secundare; evaluare de impact la prelucrarea pe scară largă.
Pacienți cu notorietate publică și angajați ai instituției	Marcaj special în sistem, cu alertă la fiecare accesare; audit periodic dedicat; un singur purtător de cuvânt desemnat.

Documentele care ajung la terți — certificate, trimiteri, bonuri de plată — se redactează astfel încât să nu dezvăluie categoria de afecțiune.

5.2. Cercetarea în domeniul sănătății

Prelucrarea datelor în scopuri de cercetare este permisă numai cu garanții suplimentare, cu respectarea normelor bioetice și a avizului comitetului de etică.

- datele se pseudonimizează sau se anonimizează ori de câte ori scopul cercetării poate fi atins astfel;
- consimțământul pentru participarea la un studiu este distinct de consimțământul pentru tratament și poate fi retras oricând;
- publicarea rezultatelor nu permite reidentificarea participanților;
- pentru statistică și managementul calității datele se utilizează agregate, cu separarea identificatorilor direcți de seturile analitice; exportul ad-hoc de fișiere cu identificatori direcți se descurajează tehnic și procedural.

Pseudonimizare și anonimizare

Pseudonimizarea înlocuiește datele de identificare cu un cod, cheia fiind păstrată separat — datele rămân date cu caracter personal. Anonimizarea elimină ireversibil posibilitatea de identificare — rezultatul nu mai constituie date cu caracter personal.

5.3. Transmiterea datelor și transferurile în afara țării

Transmiterea datelor între operatori se realizează în temeiul unui motiv legal, cu respectarea minimizării și pe canale securizate. Se transmit numai datele necesare scopului, iar destinatarul se verifică în prealabil.

Înainte de contractarea unui serviciu de tip cloud sau a unui suport tehnic din străinătate, instituția distinge între trei situații și le documentează separat în registrul evidențelor: găzduirea tehnică a datelor, accesul de mentenanță de la distanță și transferul propriu-zis către un alt operator sau împuternicit. Accesul de la distanță al furnizorului din afara țării constituie acces transfrontalier și se tratează ca atare.

Transmiterea datelor de sănătate în afara Republicii Moldova se realizează numai cu respectarea regimului legal aplicabil transferurilor transfrontaliere: decizie privind nivelul adecvat de protecție, clauze contractuale standard ori alte garanții adecvate sau, în situații determinate, derogările prevăzute de lege.

Recomandare

Pentru serviciile de tip cloud se preferă găzduirea în țară, iar locația efectivă de stocare a datelor se verifică contractual, nu se presupune.

5.4. Solicitățile autorităților și ale terților

Datele pacientului se comunică unui terț numai în temeiul legii sau cu acordul pacientului, pe baza unei cereri scrise și motivate, în limita strictă a ceea ce este necesar. Fiecare comunicare se consemnează: cine a solicitat, în ce temei, ce date au fost transmise, cine a aprobat și la ce dată. În caz de dubiu, datele nu se comunică până la clarificare.

Cine solicită	Ce se verifică	Ce se transmite
Procuror sau instanță de judecată	Ordonanța ori încheierea; persoana și obiectul indicate	Copii ale documentelor indicate, pe bază de proces-verbal.
Poliția, în afara unui dosar penal	Temeiul legal expres invocat	Numai datele strict necesare scopului invocat; în lipsa temeiului, refuz motivat.
CNAM, ANSP, alte autorități	Norma care instituie raportarea	Setul de date prevăzut de normă, în formatul stabilit.
Angajator	Existența unui temei legal sau a acordului scris	Concluzia privind aptitudinea de muncă sau documentul prevăzut de lege, niciodată diagnosticul.
Asigurător, bancă, notar	Acordul scris al pacientului	Numai datele acoperite de acord.
Rudă sau aparținător	Acordul pacientului, procura ori calitatea de reprezentant legal	Potrivit pct. 3.3. În lipsa dovezii, refuz motivat.
Instituții de presă	Acordul scris al pacientului	Nimic, în lipsa acordului. Nici măcar confirmarea prezenței.

Nu se comunică date în baza unei solicitări verbale sau telefonice, indiferent de urgența invocată. Se eliberează copii, nu originale. Comunicarea publică se realizează de o singură persoană desemnată.

5.5. Datele cu caracter personal ale personalului

Personalul instituției este, la rândul său, persoană vizată. Aceleași principii se aplică prelucrărilor din raporturile de muncă, iar angajatul are dreptul de a fi informat cu privire la ele (formularul F-02).

Prelucrare	Reguli aplicabile	Limite
Dosarul personal	Acces restrâns nominal; păstrare în spațiu securizat	Nu conține date de sănătate în afara celor prevăzute de lege.
Examenul medical la angajare și periodic	Documentația se păstrează la medicul de medicina muncii	Angajatorul primește exclusiv concluzia privind aptitudinea de muncă.
Certificatele de concediu medical	Se prelucrează pentru evidență și decontare	Angajatorul nu are acces la diagnostic.
Control acces și evidența timpului de muncă	Scop determinat, date minime	Datele biometrice necesită temei distinct și evaluare de impact.
Videosupraveghere	Potrivit pct. 4.7.	Nu se utilizează pentru evaluarea performanței.
Jurnalele de acces în sistemele informaționale	Se utilizează pentru verificarea legitimității accesărilor și pentru audit	Nu constituie instrument de monitorizare generalizată a productivității; verificările se fac pe bază de sesizare, alertă sau plan de audit aprobat.

CAPITOLUL VI. INCIDENTELE DE SECURITATE ȘI RĂSPUNDEREA

6.1. Gestionarea incidentelor de securitate

Un incident de securitate presupune pierderea, distrugerea, alterarea, divulgarea ori accesul neautorizat la date — de exemplu, pierderea unui dispozitiv, expedierea eronată a unui mesaj sau un atac informatic. Promptitudinea reacției este factorul determinant în limitarea consecințelor.

Notificarea către CNPDCP se face fără întârziere nejustificată și, în măsura posibilului, în cel mult 72 de ore de la luarea la cunoștință, atunci când incidentul este susceptibil să genereze un risc pentru drepturile persoanelor vizate. Persoanele vizate se informează atunci când riscul este ridicat.

1	Detecția	Orice angajat care observă sau suspectează un incident îl raportează imediat responsabilului cu protecția datelor sau superiorului ierarhic.
2	Evaluarea	Se stabilesc categoriile de date afectate, numărul persoanelor vizate, natura încălcării și consecințele posibile.
3	Limitarea	Izolarea sistemelor afectate, blocarea conturilor compromise, schimbarea credențialelor, recuperarea echipamentelor sau documentelor.
4	Notificarea	Dacă incidentul este susceptibil să genereze un risc, se notifică CNPDCP în cel mult 72 de ore (formularul F-12).
5	Informarea persoanelor	Dacă riscul este ridicat, persoanele afectate se informează fără întârziere, în limbaj clar.
6	Documentarea	Toate incidentele, notificate sau nu, se consemnează în registrul incidentelor.
7	Analiza ulterioară	Se identifică cauzele și se stabilesc măsuri preventive.

6.2. Consecințele neconformității

Nerespectarea obligațiilor privind protecția datelor atrage consecințe cumulative: pentru instituție, ca operator; pentru conducere, ca titular al răspunderii de management; și pentru angajatul care a săvârșit fapta.

Legea nr. 195/2024 instituie un regim de sancțiuni pecuniare aplicate direct de autoritatea de supraveghere, structurat pe două praguri: unul inferior, pentru încălcări privind evidențele, documentarea și contractele cu împuterniciții, și unul superior, pentru încălcarea principiilor de prelucrare, a drepturilor persoanelor vizate și a regulilor privind transferurile transfrontaliere.

Cuantumurile exacte și regimul de aplicare etapizată se preiau din textul în vigoare al Legii nr. 195/2024 la data aprobării ghidului și se actualizează la fiecare revizuire.

Autoritatea de supraveghere dispune, suplimentar, de măsuri corective: avertisment, mustrare, ordin de conformare, limitarea temporară sau definitivă a prelucrării, suspendarea fluxurilor de date.

Accesarea nejustificată a documentației, divulgarea informației către persoane neautorizate sau utilizarea canalelor neaprobrate constituie abateri disciplinare, independent de existența unui prejudiciu. Pacientul prejudiciat poate solicita despăgubiri, iar faptele grave pot atrage răspunderea contravențională sau penală.

Element demonstrabil	Efect în caz de control sau incident
Registrul evidențelor actualizat	Prima solicitare a autorității; absența lui este constatată imediat.
Evidența instruirilor și angajamentele semnate	Demonstrează diligența instituției și individualizează răspunderea.
Contracte de prelucrare cu toți furnizorii	Elimină cea mai frecventă neconformitate structurală.

Element demonstrabil	Efect în caz de control sau incident
Jurnalizarea accesărilor și auditul periodic	Permite identificarea rapidă a autorului și limitarea consecințelor.
Procedura de incident aplicată și documentată	Notificarea în termen reduce semnificativ gravitatea.
Evaluări de impact pentru prelucrările cu risc ridicat	Condiție de legalitate pentru dosarul electronic, telemedicină și cloud.

CAPITOLUL VII. INSTRUMENTE DE APLICARE

7.1. Situații practice

Cele 32 de situații de mai jos acoperă cazurile frecvente din activitatea curentă. Pentru fiecare sunt indicate acțiunile permise, acțiunile nepermise și recomandarea operațională. Soluțiile au caracter orientativ; deciziile care depășesc conduita curentă se iau cu avizul responsabilului cu protecția datelor.

a) Accesul la documentația pacientului

Situația	Permis	Nepermis	Recomandare operațională
1. Accesul echipei la documentația unui pacient internat	Accesul personalului implicat direct în îngrijire; accesul studenților sub supraveghere, în scop didactic justificat	Consultarea de către personal neimplicat în îngrijire	Limitarea accesului la echipa de îngrijire; documentarea accesului didactic.
2. Pacientul cere copia propriei documentații	Eliberarea copiei, după verificarea identității	Refuzul accesului; includerea datelor referitoare la alte persoane	Aplicarea procedurii de la pct. 3.2; medierea de către medic a comunicării unui diagnostic sever.
3. Aparținător care solicită documentația unui adult	Eliberarea numai cu acordul scris al pacientului sau în baza unei procuri	Comunicarea datelor pe simplul considerent al legăturii de rudenie	Solicitarea acordului scris; verificarea identității solicitantului.
4. Reprezentant legal al unei persoane fără capacitate	Eliberarea după verificarea calității, pe bază de documente	Comunicarea datelor oricărei rude, în absența dovezii	Păstrarea la dosarul cererii a copiei documentelor care atestă reprezentarea.
5. Cerere de ștergere a unui diagnostic	Examinarea cererii împreună cu responsabilul cu protecția datelor; rectificarea unei erori	Ștergerea unui diagnostic corect, la simpla cerere	Răspuns motivat: arhivarea legală și interesul de sănătate publică limitează ștergerea.
6. Documentația unei persoane cunoscute	Nicio acțiune: în absența implicării în îngrijire, accesul nu este permis	Consultarea documentației, chiar fără transmiterea informației	Îndrumarea persoanei interesate către procedura oficială de acces.

b) Urgențe și comunicarea cu pacientul

Situația	Permis	Nepermis	Recomandare operațională
7. Pacient în imposibilitate de a consimți, adus la urgență	Prelucrarea datelor și acordarea îngrijirii, în temeiul protejării intereselor vitale	Amânarea îngrijirii pentru obținerea unui consimțământ formal	Consemnarea intervenției și a temeiului; completarea formularului F-13.
8. Comunicarea rezultatelor	Comunicarea directă către pacient, după verificarea identității	Comunicarea către alte persoane; afișarea rezultatelor la ghișeu	Stabilirea anticipată a modalității: în persoană, portal securizat, plic închis.
9. Transmiterea rezultatelor prin poșta electronică	Transmiterea prin adresa instituțională, cu document protejat	Transmiterea necriptată, de pe adrese personale	Confirmarea adresei cu pacientul; utilizarea portalului securizat.
10. Solicitare prin aplicație publică de mesagerie	Informații generale, fără date de sănătate — de exemplu, orarul	Transmiterea de diagnostice, rezultate sau imagini medicale	Redirecționarea către canalele oficiale.
11. Solicitări telefonice de informații	Numai informațiile permise de procedură, după verificarea calității solicitantului	Confirmarea internării sau a diagnosticului oricărui apelant	În caz de dubiu, nedivulgarea informației.

c) Comunicarea între profesioniști, imagini, didactic

Situația	Permis	Nepermis	Recomandare operațională
12. Grupuri de mesagerie ale personalului	Discuții organizatorice care nu identifică pacientul	Publicarea de nume, imagini, rezultate sau diagnostice	Utilizarea sistemelor instituționale pentru cazuri clinice.
13. Transmiterea imagisticii către altă instituție	Transmiterea pe canal securizat, către personalul implicat în îngrijire	Transmiterea pe canale necontrolate sau către destinatari neverificați	Confirmarea destinatarului.
14. Schimbul de date între instituții	Schimbul datelor necesare îngrijirii, în temei legal și pe canale securizate	Transmiterea unui volum excesiv	Stabilirea în scris a datelor, scopului și modalității.
15. Fotografii medicale	Fotografierea cu echipament instituțional și stocarea în sistemul securizat	Utilizarea echipamentelor personale	Acordul pacientului (formularul F-03); păstrarea exclusiv în sistemul medical.
16. Prezentarea unui caz în scop didactic sau public	Materiale complet anonimizate	Prezentarea de detalii prin care pacientul poate fi recunoscut, fără temei	Aviz intern; consimțământ explicit când anonimizarea nu este posibilă.

d) Furnizori, platforme și acces tehnic

Situația	Permis	Nepermis	Recomandare operațională
17. Laborator extern care prelucrează probe	Colaborarea în temeiul unui contract de prelucrare	Transmiterea probelor în absența unui contract	Încheierea contractului anterior începerii colaborării (formularul F-09).
18. Furnizor TIC cu acces la sistem	Acces strict pentru mentenanță, în temeiul unui contract	Acces nelimitat sau permanent	Jurnalizarea intervențiilor; verificarea locației de stocare.
19. Platformă găzduită în afara țării	Utilizarea numai cu garanții de transfer și evaluare de impact	Utilizarea fără cunoașterea locației efective de stocare	Preferința pentru găzduire în țară; consultarea responsabilului cu protecția datelor.
20. Înregistrarea unei consultații la distanță	Numai conform cadrului normativ	Înregistrarea fără informarea și acordul pacientului	Informarea asupra scopului și a duratei de păstrare.
21. Accesul personalului tehnic la documentație	Acces pentru administrare, jurnalizat	Consultarea conținutului clinic în afara scopului de administrare	Control pe rol; instruire privind secretul medical.

e) Solicitări ale terților și cercetare

Situația	Permis	Nepermis	Recomandare operațională
22. Certificat solicitat de angajator	Eliberarea numai a concluziei necesare, în limita legii	Comunicarea diagnosticului către angajator	Transmiterea strictului necesar.
23. Examenul medical periodic — informația către angajator	Comunicarea exclusiv a concluziei privind aptitudinea de muncă	Transmiterea documentației medicale complete	Păstrarea separată de dosarul de personal.
24. Solicitare a unei autorități	Eliberarea numai în temeiul legii, pe baza unei cereri scrise și motivate	Predarea datelor în temeiul unei solicitări verbale	Solicitarea cererii în scris; aplicarea pct. 5.4 și a formularului F-07.

Situația	Permis	Nepermis	Recomandare operațională
25. Cercetare pe date de pacienți	Punerea la dispoziție numai pseudonimizat sau anonimizat, cu aviz etic	Furnizarea unor baze de date nominale	Implicarea comitetului de etică și a responsabilului cu protecția datelor.
26. Studiu clinic — consimțământul	Includerea numai după consimțământul informat, distinct de cel pentru tratament	Utilizarea datelor în absența unui consimțământ specific	Garantarea dreptului de retragere în orice moment.

f) Categoriile speciale, incidente și tehnologii

Situația	Permis	Nepermis	Recomandare operațională
27. Datele unui pacient decedat	Acordarea accesului în condițiile legislației aplicabile	Tratarea datelor ca informație lipsită de protecție	Aplicarea regulilor privind accesul succesorilor; menținerea secretului medical.
28. Datele minorilor	Prelucrarea pentru îngrijire, cu implicarea reprezentantului legal	Prelucrarea în servicii digitale fără temei și fără verificări	Garantii sporite; adaptarea comunicării la nivelul de înțelegere al minorului.
29. Pierderea unui dispozitiv cu date	Sesizarea imediată a responsabilului cu protecția datelor și a structurii informatice	Temporizarea sesizării	Cripare și ștergere la distanță; raportare în primele ore.
30. Mesaj expediat eronat	Tratarea ca incident; solicitarea ștergerii de către destinatar	Ignorarea situației	Evaluarea riscului; verificarea destinatarilor înainte de expediere.
31. Distrugerea documentelor pe suport de hârtie	Distrugerea securizată, prin tocare, pe bază de proces-verbal	Eliminarea la deșeurile obișnuite	Asigurarea echipamentelor de distrugere; formularul F-19.
32. Dispozitive portabile și aplicații de sănătate	Utilizarea clinică a datelor cu acordul pacientului, pe sisteme sigure	Conectarea unor dispozitive neverificate la sistemul medical	Evaluarea riscurilor; integrarea numai a soluțiilor avizate.

7.2. Întrebări frecvente

1. Este necesar consimțământul pacientului pentru prelucrarea datelor în scopul tratamentului?

În îngrijirea curentă prelucrarea se întemeiază pe necesitatea acordării asistenței medicale, pe stabilirea diagnosticului și a tratamentului sau pe obligații legale. Consimțământul informat pentru actul medical rămâne o cerință separată și la discreția instituției.

2. Are instituția obligația de a desemna un responsabil cu protecția datelor?

Da. Instituțiile care prelucrează date de sănătate la scară largă și autoritățile din domeniu desemnează un responsabil cu protecția datelor. Instituțiile mici pot desemna un responsabil partajat.

3. În ce termen se notifică un incident de securitate?

Procedura internă se activează imediat. Notificarea către CNPDCP se face fără întârziere nejustificată și, în măsura posibilului, în cel mult 72 de ore de la luarea la cunoștință. Persoanele vizate se informează atunci când riscul este ridicat.

4. Poate fi ștearsă integral documentația medicală a unui pacient, la cerere?

De regulă, nu. Obligațiile legale de arhivare și interesul de sănătate publică limitează dreptul la ștergere. Cererea se analizează, iar refuzul se motivează în scris.

5. Pot fi transmise rezultate prin aplicații publice de mesagerie?

Nu. Astfel de canale nu oferă garanțiile necesare datelor de sănătate. Se utilizează canalele securizate ale instituției.

6. Sunt protejate datele unui pacient decedat?

Da, în limitele legislației naționale. Secretul medical și normele sectoriale continuă să protejeze informațiile pacientului decedat.

7. O instituție medicală mică are obligația de a ține registrul evidențelor?

Da. Derogarea aplicabilă entităților mici nu operează atunci când se prelucrează în mod curent date de sănătate, ceea ce este propriu oricărei unități medicale.

8. Ce fac dacă un coleg îmi cere să caut ceva în documentația unei cunoștințe?

Se refuză. Accesarea în afara implicării în îngrijire constituie abatere, atât pentru cel care accesează, cât și pentru cel care solicită. Persoana interesată este îndrumată către procedura oficială de acces.

9. Pot păstra pe telefonul personal fotografia unei leziuni, pentru comparație la controlul următor?

Nu. Fotografiiile clinice se realizează cu echipament instituțional și se stochează exclusiv în sistemul medical. Ștergerea din galeria telefonului nu este suficientă, întrucât imaginile pot fi deja sincronizate în servicii externe.

10. Cine răspunde dacă un angajat accesează nejustificat documentația dintr-un sistem național?

Instituția, în calitate de operator care a acordat și a administrat dreptul de acces, împreună cu angajatul care a efectuat accesarea. Accesarea este vizibilă pacientului în istoricul accesului.

7.3. Autoevaluarea conformității

Autoevaluarea se realizează cel puțin o dată pe an, de responsabilul cu protecția datelor, și se prezintă conducerii instituției. Grila completă, cu dovada cerută, responsabilul, termenul și nivelul de maturitate pentru fiecare element, este prevăzută în formularul F-15.

Verificarea zilnică a fiecărui angajat se reduce la șase reguli:

- accesez exclusiv documentația pacienților aflați în îngrijirea mea;
- nu divulg informații despre pacienți unor persoane neautorizate;
- nu transmit date prin canale necontrolate;
- blochez sesiunea la părăsirea postului de lucru;
- distrug securizat documentele cu date;
- sesizez de îndată orice posibil incident.

7.4. Aplicarea și actualizarea ghidului

Ghidul se aplică de la data prevăzută în ordinul de aprobare. Instituțiile medico-sanitare îl preiau prin ordin intern, desemnează persoana responsabilă de implementare și completează formularele din anexa nr. 2 care le sunt aplicabile. Traseul de implementare pentru instituțiile care încep de la zero este prevăzut în formularul F-16.

Ghidul se revizuieste ori de câte ori intervin modificări ale cadrului normativ, orientări noi ale autorității de supraveghere sau schimbări semnificative ale sistemelor informaționale naționale. Observațiile și situațiile practice noi se transmit Ministerului Sănătății și pot fi incluse la pct. 7.1 la revizuirea următoare.

Revizuirea se corelează cu etapele de implementare a Programului național pentru digitalizare și inovare în sănătate pe anii 2025–2030, aprobat prin Hotărârea Guvernului nr. 556/2025 — în special cu punerea în

funcțiune a dosarului electronic de sănătate (DES), cu extinderea telemedicinii și cu dezvoltarea interoperabilității, precum și cu evoluția acțiunilor din anexa B la capitolul 28 al Programului național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025–2029, aprobat prin Hotărârea Guvernului nr. 306/2025.

GLOSAR

Termen	Definiție
Date cu caracter personal	Orice informație privind o persoană fizică identificată sau identificabilă.
Date privind sănătatea	Date referitoare la starea de sănătate fizică sau mintală, inclusiv la acordarea asistenței medicale.
Categorii speciale de date	Datele privind sănătatea, datele genetice și datele biometrice prelucrate pentru identificarea unică.
Operator	Entitatea care stabilește scopurile și mijloacele prelucrării — instituția medico-sanitară.
Persoană împuternicită de operator	Entitatea care prelucrează datele în numele operatorului — laborator, furnizor informatic, serviciu de arhivare.
Persoană vizată	Persoana ale cărei date sunt prelucrate — pacientul, angajatul.
Pseudonimizare	Prelucrare astfel încât datele să nu mai poată fi atribuite unei persoane fără informații suplimentare, păstrate separat. Datele rămân date cu caracter personal.
Anonimizare	Eliminarea ireversibilă a posibilității de identificare. Rezultatul nu mai constituie date cu caracter personal.
Incident de securitate	Încălcare care duce la distrugerea, pierderea, alterarea ori divulgarea neautorizată a datelor sau la accesul neautorizat la acestea.
Evaluarea impactului	Analiza prealabilă a riscurilor pentru drepturile persoanelor vizate, obligatorie pentru prelucrările susceptibile să genereze un risc ridicat.
Protecția datelor prin proiectare și în mod implicit	Integrarea măsurilor de protecție în arhitectura sistemului, din etapa de proiectare, cu setările cele mai protectoare active implicit.
Jurnalizare	Înregistrarea automată și nemodificabilă a operațiunilor: cine, ce, când și asupra cărei documentații.
Acces în regim de urgență	Acces care depășește temporar restricțiile obișnuite, permis numai cu justificare obligatorie, alertă și verificare ulterioară.

FORMULARE ȘI MATERIALE DE AFIȘARE

Formularele completabile și materialele de afișare constituie anexa nr. 2 la ordinul de aprobare. Instituția completează câmpurile marcate cu paranteze drepte, aprobă documentele prin ordin intern și le pune în aplicare. Un exemplar din fiecare formular completat se păstrează la responsabilul cu protecția datelor, ca element de demonstrare a conformității.

A. Formulare completabile

Cod	Denumire	Destinație
F-01	Notă de informare a pacientului	Se înmânează la prima adresare și se afișează în spațiile de primire.
F-02	Notă de informare pentru personal	Se înmânează la angajare, împreună cu angajamentul de confidențialitate.

Cod	Denumire	Destinație
F-03	Formulare de consimțământ	Trei formulare distincte: fotografii clinice; prezentare de caz și publicare; participare la un studiu.
F-04	Cerere de exercitare a drepturilor	Se pune la dispoziția pacienților la registratură și pe pagina web a instituției.
F-05	Model de răspuns și de refuz motivat	Se utilizează la soluționarea cererilor persoanelor vizate.
F-06	Registrul cererilor persoanelor vizate	Se ține de responsabilul cu protecția datelor; element de demonstrare a conformității.
F-07	Formular de eliberare a documentației către terți	Se completează la fiecare eliberare către aparținători, reprezentanți legali, succesori sau autorități.
F-08	Angajament de confidențialitate	Patru variante: personal medical, personal tehnic, studenți și rezidenți, prestatori externi.
F-09	Clauzele minime ale contractului de prelucrare	Se utilizează la contractarea laboratoarelor, furnizorilor informatici și serviciilor de arhivare.
F-10	Registrul evidențelor activităților de prelucrare	Model precompletat pentru o instituție medico-sanitară; se personalizează și se aprobă de conducere.
F-11	Evaluarea impactului asupra protecției datelor	Grila de determinare a necesității evaluării și structura raportului.
F-12	Notificarea incidentului și registrul incidentelor	Fișa de notificare, arborele de decizie privind notificarea și registrul incidentelor.
F-13	Fișă de acces în regim de urgență	Se completează în cel mult 24 de ore de la fiecare acces de urgență în sistemul informațional.
F-14	Matricea de acces pe roluri	Stă la baza configurării drepturilor în sistemele informaționale; se revizuieste semestrial.
F-15	Grilă de autoevaluare a conformității	Se completează anual de responsabilul cu protecția datelor și se prezintă conducerii.
F-16	Plan de implementare 30 / 60 / 90 de zile	Traseu pentru instituțiile care încep implementarea; se aprobă de conducere.
F-17	Registrul instruirilor și test de evaluare	Evidența instruirilor, testul de 20 de întrebări și grila de răspunsuri.
F-18	Videosupraveghere: decizie, informare, registru	Decizia de instalare, nota de informare și registrul vizionărilor.
F-19	Proces-verbal de distrugere securizată	Se întocmește la fiecare eliminare de documente cu date, pe suport de hârtie sau electronic.

B. Materiale de afișare

Se tipăresc în formatul indicat și se afișează la locul de muncă. Fiecare conține un spațiu pentru datele de contact ale responsabilului cu protecția datelor din instituție, care se completează înainte de tipărire.

Cod	Denumire	Format	Loc de afișare
M-01	Cele șase reguli de aur	A3	Cabinete, posturi de asistent, camere de gardă
M-02	Documentația unei persoane cunoscute	A3	Toate secțiile, lângă stațiile de lucru
M-03	Conduita la telefon	A4	Lângă fiecare telefon: registratură, secții, camera de gardă
M-04	Canale interzise pentru datele de pacient	A3	Secții, laborator, imagistică
M-05	Reacția la incident	A3	Toate spațiile de lucru

Cod	Denumire	Format	Loc de afișare
M-06	Birou ordonat, ecran blocat	A4	Lângă fiecare stație de lucru și imprimantă
M-07	Drepturile pacientului asupra datelor medicale	A3	Sala de așteptare, recepție
M-08	Documentele pe suport de hârtie	A4	Lângă tocător, arhivă, coșurile de birou
M-09	Acces în regim de urgență	A3	Camera de gardă, unitatea de primiri urgente
M-10	Fotografii clinice	A4	Secții chirurgicale, dermatologie, sala de pansamente
M-11	Studenți și rezidenți	A3	Clinici universitare, săli de curs clinic

Anexa nr. 2
la Ordinul ministrului sănătății nr. _____ din _____ 2026



MINISTERUL SĂNĂTĂȚII AL REPUBLICII MOLDOVA

FORMULARE ȘI MATERIALE DE AFIȘARE

la Ghidul privind protecția datelor cu caracter personal în domeniul sănătății

Chișinău, 2026

CUPRINSUL ANEXEI NR. 2

Instituția completează câmpurile marcate cu paranteze drepte, aprobă formularele prin ordin intern și le pune în aplicare. Materialele de afișare se tipăresc în formatul indicat și se amplasează la locul de muncă.

A. Formulare completabile

Cod	Denumire	Destinație
F-01	Notă de informare a pacientului	Se înmânează la prima adresare și se afișează în spațiile de primire.
F-02	Notă de informare pentru personal	Se înmânează la angajare, împreună cu angajamentul de confidențialitate.
F-03	Formulare de consimțământ	Trei formulare distincte: fotografii clinice; prezentare de caz și publicare; participare la un studiu.
F-04	Cerere de exercitare a drepturilor	Se pune la dispoziția pacienților la registratură și pe pagina web a instituției.
F-05	Model de răspuns și de refuz motivat	Se utilizează la soluționarea cererilor persoanelor vizate.
F-06	Registrul cererilor persoanelor vizate	Se ține de responsabilul cu protecția datelor; element de demonstrare a conformității.
F-07	Formular de eliberare a documentației către terți	Se completează la fiecare eliberare către aparținători, reprezentanți legali, succesori sau autorități.
F-08	Angajament de confidențialitate	Patru variante: personal medical, personal tehnic, studenți și rezidenți, prestatori externi.
F-09	Clauzele minime ale contractului de prelucrare	Se utilizează la contractarea laboratoarelor, furnizorilor informatici și serviciilor de arhivare.
F-10	Registrul evidențelor activităților de prelucrare	Model precompletat pentru o instituție medico-sanitară; se personalizează și se aprobă de conducere.
F-11	Evaluarea impactului asupra protecției datelor	Grila de determinare a necesității evaluării și structura raportului.
F-12	Notificarea incidentului și registrul incidentelor	Fișa de notificare, arborele de decizie privind notificarea și registrul incidentelor.
F-13	Fișă de acces în regim de urgență	Se completează în cel mult 24 de ore de la fiecare acces de urgență în sistemul informațional.
F-14	Matricea de acces pe roluri	Stă la baza configurării drepturilor în sistemele informaționale; se revizuieste semestrial.
F-15	Grilă de autoevaluare a conformității	Se completează anual de responsabilul cu protecția datelor și se prezintă conducerii.
F-16	Plan de implementare 30 / 60 / 90 de zile	Traseu pentru instituțiile care încep implementarea; se aprobă de conducere.
F-17	Registrul instruirilor și test de evaluare	Evidența instruirilor, testul de 20 de întrebări și grila de răspunsuri.
F-18	Videosupraveghere: decizie, informare, registru	Decizia de instalare, nota de informare și registrul vizionărilor.
F-19	Proces-verbal de distrugere securizată	Se întocmește la fiecare eliminare de documente cu date, pe suport de hârtie sau electronic.

B. Materiale de afișare

Cod	Denumire	Format	Loc de afișare
M-01	Cele șase reguli de aur	A3	Cabinete, posturi de asistent, camere de gardă
M-02	Documentația unei persoane cunoscute	A3	Toate secțiile, lângă stațiile de lucru
M-03	Conduita la telefon	A4	Lângă fiecare telefon: registratură, secții, camera de gardă
M-04	Canale interzise pentru datele de pacient	A3	Secții, laborator, imagistică
M-05	Reacția la incident	A3	Toate spațiile de lucru
M-06	Birou ordonat, ecran blocat	A4	Lângă fiecare stație de lucru și imprimantă
M-07	Drepturile pacientului asupra datelor medicale	A3	Sala de așteptare, recepție
M-08	Documentele pe suport de hârtie	A4	Lângă tocător, arhivă, coșurile de birou
M-09	Acces în regim de urgență	A3	Camera de gardă, unitatea de primiri urgente
M-10	Fotografii clinice	A4	Secții chirurgicale, dermatologie, sala de pansamente
M-11	Studenți și rezidenți	A3	Clinici universitare, săli de curs clinic

Formularul F-01

NOTĂ DE INFORMARE A PACIENTULUI

Se înmânează la prima prezentare și se afișează în spațiile de primire. Câmpurile marcate cu paranteze drepte se completează de instituție.

Instituția medico-sanitară	[denumirea completă]
Sediul	[adresa]
Responsabilul cu protecția datelor	[nume, telefon, e-mail]

1. Cine prelucrează datele dumneavoastră

Operatorul de date este [denumirea instituției], cu sediul în [adresă], reprezentată prin [funcția conducătorului]. Puteți contacta responsabilul cu protecția datelor la [e-mail] sau la [telefon].

2. În ce scopuri și în ce temei

Scopul prelucrării	Temeiul	Este necesar acordul dumneavoastră?
Acordarea asistenței medicale: consultație, diagnostic, tratament, îngrijire	Necesitatea acordării asistenței medicale	Nu
Raportări și decontări obligatorii către CNAM, ANSP și alte autorități	Obligație legală a instituției	Nu
Îngrijirea în situații de urgență, când nu vă puteți exprima voința	Protejarea intereselor vitale	Nu
Supravegherea epidemiologică a bolilor transmisibile	Interes public în domeniul sănătății publice	Nu
Fotografii clinice, prezentări de caz, publicare	Consimțământul dumneavoastră	Da
Înregistrarea unei teleconsultații	Consimțământul dumneavoastră	Da
Participarea la un studiu de cercetare	Consimțământul dumneavoastră, cu aviz etic	Da

Prelucrările care necesită acordul dumneavoastră sunt facultative. Refuzul nu afectează în niciun fel accesul la serviciile medicale, iar acordul poate fi retras oricând.

3. Ce categorii de date prelucram

Date de identificare (nume, prenume, IDNP, buletin de identitate), date de contact, date privind starea de sănătate (diagnostic, tratament, investigații, istoric medical), date privind asigurarea medicală și, după caz, date financiare pentru decontări.

4. Cine mai are acces la datele dumneavoastră

- personalul medical implicat direct în îngrijirea dumneavoastră, supus obligației secretului profesional;
- laboratoarele și furnizorii de servicii cu care instituția are contracte de prelucrare;

- Compania Națională de Asigurări în Medicină și autoritățile de sănătate publică, în limitele raportărilor obligatorii;
- alte instituții medicale, atunci când sunteți transferat sau când continuitatea îngrijirii o impune;
- autoritățile competente, numai în temeiul legii și pe baza unei cereri scrise și motivate.

5. Sistemele informaționale naționale

Datele dumneavoastră pot fi înregistrate în sistemele informaționale naționale de sănătate, între care dosarul electronic de sănătate, eRețeta și Portalul certificatelor de concediu medical. Puteți consulta oricând istoricul accesărilor la propria documentație, prin serviciile guvernamentale disponibile.

6. Cât timp păstrăm datele

Datele se păstrează pe durata prevăzută de reglementările privind documentația medicală și de nomenclatorul dosarelor aprobat al instituției. La expirarea termenului, datele se șterg sau se anonimizează.

7. Transferuri în afara Republicii Moldova

Datele nu se transmit în afara Republicii Moldova decât în condițiile prevăzute de lege și numai cu garanții adecvate de protecție.

8. Drepturile dumneavoastră

Dreptul	Ce înseamnă
Informare	Să știți ce date prelucrăm, în ce scop și cine le poate vedea.
Acces	Să primiți o copie a datelor dumneavoastră medicale.
Rectificare	Să cereți corectarea datelor inexacte sau completarea celor incomplete.
Ștergere	Să cereți ștergerea datelor. În domeniul medical acest drept este limitat de obligațiile legale de arhivare și de interesul de sănătate publică.
Restricționare	Să cereți suspendarea utilizării datelor, în situațiile prevăzute de lege.
Portabilitate	Să primiți, într-un format structurat, datele pe care ni le-ați furnizat dumneavoastră.
Opoziție	Să vă opuneți unei prelucrări. Nu se aplică îngrijirii medicale și raportărilor obligatorii.
Intervenție umană	Ca o decizie automată care vă privește să fie verificată de o persoană.
Retragerea acordului	Să retrageți oricând un acord dat, la fel de simplu cum a fost acordat.

9. Cum vă exercitați drepturile

Depuneți o cerere scrisă la registratura instituției sau adresați-vă direct responsabilului cu protecția datelor, la datele de contact de mai sus. Formularul de cerere este disponibil la registratură și pe pagina web a instituției. Vă răspundem gratuit, în termen de o lună de la înregistrarea cererii. În cazuri complexe termenul poate fi prelungit, cu informarea dumneavoastră prealabilă. Un eventual refuz se motivează în scris.

Dacă apreciați că drepturile dumneavoastră au fost încălcate, vă puteți adresa Centrului Național pentru Protecția Datelor cu Caracter Personal (www.datepersonale.md) sau instanței de judecată.

Data informării ____ / ____ / _____	Semnătura de luare la cunoștință _____
--	---

Formularul F-02

NOTĂ DE INFORMARE PENTRU PERSONAL

Se înmânează la încadrare, împreună cu angajamentul de confidențialitate.

Instituția medico-sanitară	[denumirea completă]
Sediul	[adresa]
Responsabilul cu protecția datelor	[nume, telefon, e-mail]

În calitate de angajat al instituției, sunteți la rândul dumneavoastră persoană vizată. Prezenta notă vă informează cu privire la prelucrarea datelor dumneavoastră cu caracter personal în cadrul raporturilor de muncă.

1. Ce date prelucrăm și în ce scop

Categoria de date	Scopul	Cine are acces
Date de identificare, contact, studii, experiență	Încadrarea și administrarea raportului de muncă	Resurse umane, conducerea
Date de salarizare și fiscale	Salarizare, decontări, raportări obligatorii	Contabilitate, CNAS, CNAM
Concluzia de aptitudine de muncă	Respectarea obligațiilor de securitate a muncii	Resurse umane
Documentația examenului medical	Evaluarea stării de sănătate în raport cu postul	Exclusiv medicul care efectuează examenul medical
Certificate de concediu medical	Evidența timpului de muncă și decontarea indemnizațiilor	Resurse umane, contabilitate — fără acces la diagnostic
Date de control acces și pontaj	Evidența prezenței și securitatea spațiilor	Administrativ, resurse umane
Imagini de videosupraveghere	Securitatea persoanelor și a bunurilor	Persoanele desemnate nominal
Jurnalele de acces în sistemele informaționale	Verificarea legitimității accesărilor și auditul de securitate	IT, responsabilul cu protecția datelor
Evidența instruirilor	Demonstrarea conformității	Resurse umane, responsabilul cu protecția datelor

2. Jurnalizarea accesărilor

De reținut

Fiecare accesare pe care o efectuați în sistemele informaționale medicale este înregistrată automat: cine, ce documentație, când și ce operațiune. Jurnalele se verifică pe bază de sesizare, de alertă automată sau conform planului de audit aprobat. Ele nu se utilizează pentru monitorizarea generalizată a productivității.

3. Ce nu facem

- Nu utilizăm videosupravegherea pentru evaluarea performanței dumneavoastră.
- Nu comunicăm diagnosticul dumneavoastră conducerii sau colegilor; angajatorul primește exclusiv concluzia de aptitudine.
- Nu prelucrăm date biometrice fără un temei distinct și fără o evaluare prealabilă a impactului.

4. Cât timp păstrăm datele

Dosarul personal se păstrează potrivit nomenclatorului dosarelor aprobat al instituției.

5. Drepturile dumneavoastră

Aveți aceleași drepturi ca orice persoană vizată: informare, acces, rectificare, ștergere în limitele legale, restricționare, portabilitate și opoziție. Le exercitați printr-o cerere adresată responsabilului cu protecția datelor. Vă puteți adresa și Centrului Național pentru Protecția Datelor cu Caracter Personal.

Am primit un exemplar <i>(nume, prenume, semnătura)</i>	Din partea instituției <i>(nume, prenume, semnătura)</i>
---	--

FORMULARE DE CONSIMȚĂMÂNT

Trei formulare distincte. Se tipăresc și se completează separat, în funcție de situație.

Când se folosesc aceste formulare

Numai pentru prelucrările care necesită consimțământ. Îngrijirea medicală curentă, raportările obligatorii și prelucrările impuse de lege NU necesită consimțământ pentru date — solicitarea lui în aceste situații este o eroare. Consimțământul informat pentru actul medical este o instituție distinctă și se obține separat.

Formularul 1 — Fotografii și înregistrări clinice

Instituția medico-sanitară	[denumirea completă]
Sediul	[adresa]
Responsabilul cu protecția datelor	[nume, telefon, e-mail]

Subsemnatul/a _____, IDNP _____, consimt ca instituția să realizeze fotografii sau înregistrări ale zonei/afecțiunii _____, în următoarele scopuri:

☐	documentarea evoluției clinice, exclusiv în documentația mea medicală;
☐	consult de specialitate cu alți medici implicați în îngrijirea mea;
☐	altul: _____

Am fost informat/ă că: imaginile se realizează exclusiv cu echipament al instituției și se stochează numai în sistemul medical securizat; nu se stochează pe dispozitive personale; se păstrează pe durata prevăzută pentru documentația medicală; refuzul meu nu afectează accesul la servicii medicale; îmi pot retrage acordul oricând, fără a fi nevoit să motivez.

Pacient / reprezentant legal	Cadrul medical care a informat
_____ (nume, prenume, semnătura)	_____ (nume, prenume, semnătura)

Data: ____ / ____ / ____

Formularul 2 — Prezentarea unui caz și publicare

Instituția medico-sanitară	[denumirea completă]
Sediul	[adresa]
Responsabilul cu protecția datelor	[nume, telefon, e-mail]

Subsemnatul/a _____, IDNP _____, consimt ca informațiile și materialele privind cazul meu să fie utilizate în următorul scop:

☐	prezentare în cadrul unei activități didactice interne;
☐	prezentare la o conferință sau la o manifestare științifică;
☐	publicare într-o revistă de specialitate;
☐	material de informare publică al instituției.

Am fost informat/ă că materialele vor fi anonimizate, iar elementele care ar permite recunoașterea mea vor fi eliminate. Atunci când anonimizarea completă nu este posibilă, acest lucru mi-a fost explicat, iar acordul meu se referă în mod expres la materialele care mă pot identifica.

☐	Accept utilizarea unor materiale prin care pot fi recunoscut/ă.
☐	Nu accept utilizarea unor materiale prin care pot fi recunoscut/ă.

Îmi pot retrage acordul oricând. Retragera produce efecte pentru viitor și nu afectează materialele deja publicate, dacă retragera nu mai este tehnic posibilă.

Pacient / reprezentant legal	Cadrul medical care a informat
_____	_____
(nume, prenume, semnătura)	(nume, prenume, semnătura)

Aviz intern (responsabilul cu protecția datelor): _____ **Data:** ____ / ____ / ____

Formularul 3 — Participarea la un studiu

Instituția medico-sanitară	[denumirea completă]
Sediul	[adresa]
Responsabilul cu protecția datelor	[nume, telefon, e-mail]
Denumirea studiului	[titlul complet]
Investigator principal	[nume, funcție]
Avizul comitetului de etică	nr. _____ din ____ / ____ / ____

Subsemnatul/a _____, IDNP _____, consimt să particip la studiul menționat mai sus și ca datele mele să fie prelucrate în acest scop.

Am fost informat/ă cu privire la: scopul și durata studiului; categoriile de date prelucrate; faptul că datele vor fi pseudonimizate, iar cheia de corespondență va fi păstrată separat; destinatarii datelor; durata de păstrare; eventualele transferuri în afara țării și garanțiile aplicabile; faptul că rezultatele se publică fără posibilitatea reidentificării mele.

Distinct de consimțământul pentru tratament

Acest consimțământ privește exclusiv participarea la studiu. Refuzul sau retragerea nu afectează în niciun fel îngrijirea medicală la care am dreptul. Îmi pot retrage acordul în orice moment, fără a motiva și fără nicio consecință.

Participant / reprezentant legal _____ (nume, prenume, semnătura)	Investigator _____ (nume, prenume, semnătura)
--	--

Data: ____ / ____ / ____

Formularul F-04

CERERE DE EXERCITARE A DREPTURILOR

Se pune la dispoziția pacienților la registratură și pe pagina web a instituției.

Către: [denumirea instituției medico-sanitare]

În atenția: responsabilului cu protecția datelor

I. Datele solicitantului

Nume, prenume	
IDNP	
Adresa	
Telefon	
Adresa de e-mail	

II. Calitatea în care formulez cererea

☐	Pacient — datele mele proprii
☐	Reprezentant legal al pacientului (se anexează documentele care atestă calitatea)
☐	Persoană împuternicită prin procură (se anexează procura)
☐	Succesor al pacientului decedat (se anexează documentele care atestă calitatea)

III. Dreptul pe care îl exercit

☐	Acces	Solicit o copie a datelor mele medicale
☐	Rectificare	Solicit corectarea unor date inexacte sau completarea celor incomplete
☐	Ștergere	Solicit ștergerea unor date (drept limitat în domeniul medical)
☐	Restricționare	Solicit suspendarea utilizării unor date
☐	Portabilitate	Solicit datele furnizate de mine, într-un format structurat
☐	Opoziție	Mă opun unei anumite prelucrări
☐	Intervenție umană	Solicit verificarea de către o persoană a unei decizii automate
☐	Retragerea acordului	Retrag un acord dat anterior

IV. Obiectul cererii

Datele și perioada la care se referă cererea, precum și motivul, atunci când dreptul exercitat îl presupune:

V. Modalitatea de comunicare a răspunsului

☐	Pe suport de hârtie, ridicat personal de la registratură
☐	Pe suport de hârtie, expediat prin poștă la adresa indicată
☐	În format electronic, la adresa de e-mail indicată

Solicitant _____ <i>(nume, prenume, semnătura)</i>	Am primit cererea (registratură) _____ <i>(nume, prenume, semnătura)</i>
---	---

Data: ____ / ____ / ____

Nr. de înregistrare: _____

Informații pentru solicitant

Identitatea solicitantului se verifică obligatoriu înainte de soluționare — este o măsură de protecție a datelor dumneavoastră. Cererea se soluționează gratuit, în termen de o lună de la înregistrare. În cazuri complexe termenul poate fi prelungit, cu informarea dumneavoastră prealabilă. Un eventual refuz se comunică în scris și motivat, cu indicarea dreptului de a sesiza CNPDCP.

MODEL DE RĂSPUNS ȘI DE REFUZ MOTIVAT

Se utilizează de responsabilul cu protecția datelor la soluționarea cererilor persoanelor vizate.

Modelul 1 — Răspuns favorabil

Instituția medico-sanitară	[denumirea completă]
Sediul	[adresa]
Responsabilul cu protecția datelor	[nume, telefon, e-mail]

Nr. _____ din ____ / ____ / _____

Către: [nume, prenume solicitant], [adresa]

Stimată doamnă / Stimate domn,

Ca urmare a cererii dumneavoastră înregistrate cu nr. _____ din ____ / ____ / _____, prin care ați solicitat [obiectul cererii], vă comunicăm următoarele.

Cererea a fost analizată și admisă. [Se descrie soluția: se anexează copia datelor solicitate; s-a efectuat rectificarea solicitată; s-a aplicat restricționarea etc.]

Datele comunicate se referă exclusiv la persoana dumneavoastră. Informațiile privind terțe persoane au fost eliminate, potrivit legii.

Vă stăm la dispoziție pentru orice clarificare la datele de contact indicate mai sus. Dacă apreciați că drepturile dumneavoastră nu au fost respectate, vă puteți adresa Centrului Național pentru Protecția Datelor cu Caracter Personal (www.datepersonale.md) sau instanței de judecată.

Conducătorul instituției	Responsabilul cu protecția datelor
_____	_____
(nume, prenume, semnătura)	(nume, prenume, semnătura)

Modelul 2 — Refuz motivat

Instituția medico-sanitară	[denumirea completă]
Sediul	[adresa]
Responsabilul cu protecția datelor	[nume, telefon, e-mail]

Nr. _____ din ____ / ____ / _____

Către: [nume, prenume solicitant], [adresa]

Stimată doamnă / Stimate domn,

Ca urmare a cererii dumneavoastră înregistrate cu nr. _____ din ____ / ____ / _____, prin care ați solicitat [obiectul cererii], vă comunicăm că aceasta nu poate fi admisă, pentru următoarele motive.

Motivarea: [se indică temeiul concret al refuzului — de exemplu, obligația legală de arhivare a documentației medicale, interesul de sănătate publică, protejarea drepturilor terților, imposibilitatea verificării identității sau a calității de reprezentant].

[După caz:] Deși cererea de ștergere nu poate fi admisă, aveți posibilitatea de a solicita completarea dosarului cu o declarație proprie, care va fi păstrată alături de documentația medicală.

Împotriva prezentului răspuns vă puteți adresa Centrului Național pentru Protecția Datelor cu Caracter Personal (www.datepersonale.md) sau instanței de judecată, în condițiile legii.

Conducătorul instituției	Responsabilul cu protecția datelor
_____	_____
(nume, prenume, semnătura)	(nume, prenume, semnătura)

Regulă

Orice refuz se comunică în scris, se motivează concret — nu generic — și indică întotdeauna calea de atac. Un refuz nemotivat este, el însuși, o neconformitate.

Formularul F-06

REGISTRUL CERERILOR PERSOANELOR VIZATE

Se ține de responsabilul cu protecția datelor. Element de demonstrare a conformității.

Nr.	Data primirii	Solicitant	Calitatea	Dreptul exercitat	Termen limită	Data răspunsului	Soluția	Obs.

Instrucțiuni de completare

Calitatea: pacient, reprezentant legal, împuternicit prin procură, succesor. Termenul limită se calculează ca o lună de la data primirii; prelungirea se consemnează cu indicarea motivului. Soluția: admisă, admisă parțial, respinsă — cu trimitere la numărul răspunsului. Registrul se păstrează pe durata relației cu persoana vizată și încă trei ani.

Formularul F-07

FORMULAR DE ELIBERARE A DOCUMENTAȚIEI CĂTRE TERȚI

Se completează la fiecare eliberare către aparținători, reprezentanți legali, succesori sau autorități.

Instituția medico-sanitară	[denumirea completă]
Sediul	[adresa]
Responsabilul cu protecția datelor	[nume, telefon, e-mail]

I. Pacientul la care se referă documentația

Nume, prenume	
IDNP	
Perioada / episodul de îngrijire	

II. Solicitantul și temeiul

☐	Pacientul însuși	Verificarea actului de identitate
☐	Persoană împuternicită prin procură	Se anexează procura, în original sau copie legalizată
☐	Rudă, cu acordul scris al pacientului	Se anexează acordul scris, semnat de pacient
☐	Reprezentant legal	Se anexează hotărârea judecătorească sau actul de tutelă
☐	Succesor al pacientului decedat	Se anexează certificatul de deces și dovada calității
☐	Autoritate publică	Se anexează cererea scrisă și motivată, cu indicarea temeiului legal
☐	Organ de urmărire penală sau instanță	Se anexează ordonanța, încheierea ori adresa

Nume, prenume solicitant	
IDNP / buletin de identitate	
Documentul justificativ anexat	

III. Documentele eliberate

Nr.	Denumirea documentului	Nr. de file	Copie / original
1			
2			
3			
4			
5			

Se eliberează exclusiv copii, cu excepția cazurilor prevăzute expres de lege. Se transmite numai volumul de date necesar scopului invocat.

IV. Aprobare și predare

Avizul responsabilului cu protecția datelor	
Aprobarea conducătorului instituției	
Data eliberării	

Am predat (instituția)	Am primit (solicitantul)
_____	_____
<i>(nume, prenume, semnătura)</i>	<i>(nume, prenume, semnătura)</i>

În caz de dubiu

Dacă temeiul nu este clar sau documentele justificative lipsesc, documentația NU se eliberează. Cererea se transmite responsabilului cu protecția datelor și structurii juridice, iar solicitantul este informat în scris.

Formularul F-08

ANGAJAMENT DE CONFIDENȚIALITATE

Patru variante. Se semnează la încadrare, la începerea stagiului sau la începerea colaborării.

Varianta 1 — Personal medical și administrativ

Instituția medico-sanitară	[denumirea completă]
Sediul	[adresa]
Responsabilul cu protecția datelor	[nume, telefon, e-mail]

Subsemnatul/a _____, IDNP _____, angajat/ă în funcția de _____, în cadrul subdiviziunii _____, declar că am luat cunoștință de Ghidul privind protecția datelor cu caracter personal în domeniul sănătății și de politicile interne ale instituției și mă oblig:

- să accesez exclusiv datele pacienților aflați în îngrijirea mea sau necesare exercitării atribuțiilor de serviciu;
- să nu divulg informații despre pacienți niciunei persoane neautorizate, nici în timpul, nici după încetarea raporturilor de muncă;
- să utilizez exclusiv contul propriu și să nu comunic nimănui datele de autentificare;
- să blochez sesiunea la fiecare părăsire a postului de lucru;
- să transmit date de sănătate exclusiv prin canalele instituționale aprobate, niciodată prin aplicații publice de mesagerie sau conturi personale de e-mail;
- să nu fotografiez pacienți sau documente cu dispozitive personale;
- să sesizez de îndată orice incident de securitate constatat sau suspectat;
- să restitui, la încetarea raporturilor de muncă, toate documentele și echipamentele care conțin date.

Am fost informat/ă că accesările efectuate în sistemele informaționale sunt jurnalizate și pot fi auditate, inclusiv de către pacient, și că nerespectarea prezentului angajament atrage răspunderea disciplinară, civilă, contravențională sau penală, după caz.

Angajat _____ (nume, prenume, semnătura)	Din partea instituției _____ (nume, prenume, semnătura)
---	--

Data: ____ / ____ / ____

Varianța 2 — Personal tehnic și administratori de sistem

Instituția medico-sanitară	[denumirea completă]
Sediul	[adresa]
Responsabilul cu protecția datelor	[nume, telefon, e-mail]

Subsemnatul/a _____, IDNP _____, exercitând atribuții de _____, declar că am luat cunoștință de obligațiile ce îmi revin și mă oblig, suplimentar față de obligațiile generale:

- să utilizez contul cu drepturi privilegiate exclusiv pentru sarcini de administrare și mentenanță, pe durata strict necesară și în temeiul unei autorizări documentate;
- să nu consult conținutul clinic al dosarelor în afara scopului de administrare;
- să nu dezactivez, să nu modific și să nu șterg jurnalele de acces;
- să folosesc conturi nominale, distincte de contul de utilizator curent, și să nu le partajez;
- să documentez fiecare intervenție în mediul de producție: motivul, intervalul, operațiunile efectuate;
- să respect obligația secretului profesional medical, care mi se aplică în aceeași măsură ca personalului medical.

Semnatar	Din partea instituției
_____	_____
(nume, prenume, semnătura)	(nume, prenume, semnătura)

Data: ____ / ____ / ____

Varianța 3 — Studenți, rezidenți și voluntari

Instituția medico-sanitară	[denumirea completă]
Sediul	[adresa]
Responsabilul cu protecția datelor	[nume, telefon, e-mail]

Subsemnatul/a _____, IDNP _____, student/rezident/voluntar în cadrul _____, pe perioada ____ / ____ / ____ – ____ / ____ / _____, declar că am luat cunoștință de regulile privind protecția datelor și mă oblig:

- să accesez dosarele pacienților exclusiv sub supravegherea cadrului didactic sau a medicului responsabil și numai în scop didactic justificat;
- să nu fotografiez, să nu copiez și să nu extrag date din sistemele instituției;
- să nu discut cazuri identificabile în afara activității didactice și să nu le public pe rețele sociale;
- să utilizez, în lucrări și prezentări, exclusiv materiale complet anonimizate;
- să respect secretul profesional și după încheierea stagiului.

Semnatar	Coordonator de stagi
_____	_____
(nume, prenume, semnătura)	(nume, prenume, semnătura)

Data: ____ / ____ / _____

Varianța 4 — Prestatori externi

Instituția medico-sanitară	[denumirea completă]
Sediul	[adresa]
Responsabilul cu protecția datelor	[nume, telefon, e-mail]

Subsemnatul/a _____, reprezentând _____, în temeiul contractului nr. _____ din ____ / ____ / _____, declar că mă oblig:

- să prelucrez datele exclusiv pe baza instrucțiunilor documentate ale instituției;
- să accesez mediul de producție numai punctual, pe interval limitat, cu cont nominal și aprobare prealabilă;
- să nu copiez, să nu extrag și să nu utilizez datele în scop propriu, inclusiv statistic sau de antrenare a modelelor informatice;
- să notific instituția, fără întârziere și în cel mult 24 de ore, cu privire la orice incident de securitate;
- să șterg sau să restitui datele la încetarea colaborării, cu dovadă documentată.

Reprezentantul prestatorului	Din partea instituției
_____ (nume, prenume, semnătura)	_____ (nume, prenume, semnătura)

Data: ____ / ____ / _____

Formularul F-09

CLAUZELE MINIME ALE CONTRACTULUI DE PRELUCRARE

Se utilizează la contractarea laboratoarelor, furnizorilor informatici, serviciilor de cloud, mentenanță și arhivare.

Prezenta anexă cuprinde clauzele minime care se includ în contractul încheiat cu orice persoană împuternicită. Ele se adaptează la specificul serviciului, dar niciuna nu poate lipsi.

Clauză	Conținut minim
Obiectul și durata	Operațiunile de prelucrare, categoriile de date și de persoane vizate, durata prelucrării.
Instrucțiuni	Prelucrarea se realizează exclusiv pe baza instrucțiunilor documentate ale operatorului. Orice altă prelucrare este interzisă.
Confidențialitate	Angajamente de confidențialitate semnate de tot personalul cu acces la date, păstrate de împuternicit și puse la dispoziție la cerere.
Măsuri de securitate	Măsuri concrete, nu formulări generale: criptare în tranzit și la stocare, control al accesului pe rol, autentificare cu mai mulți factori, jurnalizare, copii de rezervă testate prin restaurare.
Localizarea datelor	Țara și centrul de date în care se stochează datele; interdicția relocării fără acordul prealabil scris al operatorului.
Acces de mentenanță	Cont nominal, autentificare cu mai mulți factori, aprobare prealabilă pentru fiecare intervenție, interval limitat, înregistrarea sesiunii, revocarea drepturilor la închiderea tichetului.
Subcontractare	Numai cu acordul prealabil scris al operatorului; aceleași obligații se transmit integral subcontractantului; lista subcontractanților se menține actualizată.
Asistență	Sprijin la soluționarea cererilor persoanelor vizate, la evaluările de impact și la notificarea incidentelor, în termenele solicitate de operator.
Incidente	Notificarea operatorului fără întârziere și în cel mult 24 de ore de la constatare, cu descrierea incidentului, a datelor afectate și a măsurilor luate.
Audit	Dreptul operatorului de a audita, direct sau prin terț desemnat; punerea la dispoziție a jurnalelor de acces și a documentației de securitate.
Utilizare secundară	Interdicția expresă a oricărei utilizări în scop propriu, inclusiv statistic, comercial sau de antrenare a modelelor informatice.
Încetare	Restituirea sau ștergerea datelor, la alegerea operatorului, în termen de [] zile de la încetare, cu dovadă documentată a ștergerii, inclusiv din copiile de rezervă.
Răspundere	Răspunderea împuternicitului pentru prejudiciile cauzate prin nerespectarea obligațiilor și pentru sancțiunile suportate de operator din această cauză.

Cerințe suplimentare pentru achizițiile de sisteme informaționale

În caietele de sarcini, cerințele de protecție a datelor se formulează ca cerințe de conformitate demonstrabilă, verificabile la recepție:

- control al accesului bazat pe rol și pe atribut (tură, locație, dispozitiv, relație clinică);
- pistă de audit completă, cu export al jurnalelor în format prelucrabil;
- mecanism de acces în regim de urgență, cu justificare obligatorie și alertă automată;
- pseudonimizare a suporturilor fizice (etichete cu cod de bare în locul numelui și al IDNP);
- limitarea implicită a exporturilor și mecanisme de prevenire a scurgerilor de date;

- interoperabilitate conform standardelor HL7 FHIR, DICOM și LOINC;
- documentație de securitate și rezultatele ultimului test de securitate.

Formularul F-10

REGISTRUL EVIDENȚELOR ACTIVITĂȚILOR DE PRELUCRARE

Model precompletat pentru o instituție medico-sanitară. Se personalizează, se aprobă de conducere și se revizuieste anual.

Activitatea de prelucrare	Scopul	Categorii de date	Destinatari	Termen de păstrare	Măsurile de securitate
Registratură și programări	Programarea și evidența adresărilor	Identificare, contact, statut de asigurare	Personalul de registratură, medicul curant	Potrivit nomenclatorului	Acces pe rol, jurnalizare, blocarea sesiunii
Asistență medicală primară	Diagnostic, tratament, monitorizare	Identificare, date de sănătate	Echipa de îngrijire, CNAM	25 de ani*	Acces pe rol, jurnalizare, criptare
Asistență medicală spitalicească	Diagnostic, tratament, îngrijire	Identificare, date de sănătate	Echipa de îngrijire, CNAM, ANSP	25 de ani*	Acces pe rol și pe episod de îngrijire, jurnalizare
Laborator	Efectuarea și raportarea investigațiilor	Identificare, rezultate	Medicul solicitant, pacientul	Potrivit nomenclatorului	Pseudonimizare pe suporturi fizice, cod de bare
Imagistică (RIS/PACS)	Investigații imagistice	Identificare, imagini, rapoarte	Medicul solicitant, instituția care preia pacientul	10 ani*	Acces pe rol, transmitere pe canale securizate
Farmacie de spital	Eliberarea medicamentelor	Identificare, prescripții	Personalul farmaciei, CNAM	Potrivit nomenclatorului	Acces restrâns, evidența eliberărilor
eRețeta, PCCM, DES	Prescriere electronică, certificate, dosar electronic	Identificare, date de sănătate	Sisteme naționale, CNAM, CNAS	Potrivit regulilor sistemului	MPass/MSign, jurnalizare, istoricul accesului
Raportări obligatorii	Îndeplinirea obligațiilor legale	Seturile prevăzute de norme	CNAM, ANSP, CNEAS, MS	Potrivit normelor	Transmitere securizată, minimizare
Videosupraveghere	Securitatea persoanelor și a bunurilor	Imagini	Persoane desemnate nominal	Maximum 30 de zile	Acces nominal, registrul vizionărilor
Resurse umane	Administrarea raporturilor de muncă	Identificare, studii, salarizare, aptitudine de muncă	Contabilitate, CNAS, CNAM	75 de ani (dosar personal)	Acces restrâns, spațiu securizat
Examen medical la angajare și periodice	Evaluarea aptitudinii de muncă	Date de sănătate ale angajaților	Medicul care efectuează examenul medical	Potrivit normelor	Păstrare separată de dosarul de personal
Cereri ale persoanelor vizate	Soluționarea cererilor	Identificare, obiectul cererii	Responsabilul cu protecția datelor, structura juridică	Durata relației plus 3 ani	Registru dedicat, acces restrâns

* Termenele marcate se confirmă prin nomenclatorul dosarelor aprobat al instituției.

Întocmit: responsabilul cu protecția datelor	Aprobat: conducătorul instituției
_____ Data: ____ / ____ / ____	_____ Data: ____ / ____ / ____

Formularul F-11

EVALUAREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR

Grila de determinare a necesității evaluării și structura raportului de evaluare.

Partea I — Este necesară o evaluare de impact?

Se bifează criteriile aplicabile prelucrării analizate. Bifarea a două sau a mai multor criterii indică, de regulă, necesitatea unei evaluări de impact. În domeniul medical, prelucrarea la scară largă a datelor de sănătate este, prin ea însăși, un criteriu suficient.

	Criteriu	Aplicabil
1	Prelucrare pe scară largă a datelor privind sănătatea, genetice sau biometrice	☐
2	Interconectarea sau punerea în corespondență a mai multor seturi de date ori sisteme	☐
3	Utilizarea unei tehnologii noi: soluții de inteligență artificială pentru diagnostic, triaj sau scoring clinic	☐
4	Evaluare sistematică sau scor automat cu efect asupra deciziei clinice	☐
5	Monitorizare sistematică a unei zone accesibile publicului (videosupraveghere)	☐
6	Prelucrarea datelor persoanelor vulnerabile: minori, persoane fără discernământ, pacienți în regim special de confidențialitate	☐
7	Transfer de date în afara țării sau găzduire în afara spațiului european	☐
8	Dispozitive medicale conectate sau aplicații care transmit date către instituție	☐
9	Prelucrare care poate împiedica accesul la un serviciu sau la un drept	☐
10	Prelucrare care implică un furnizor extern cu acces la mediul de producție	☐

Prelucrarea analizată	
Numărul criteriilor bifate	
Concluzie	Evaluare de impact: ☐ necesară ☐ nu este necesară
Data și semnătura DPO	

Partea a II-a — Structura raportului de evaluare

Secțiune	Conținut
1. Descrierea prelucrării	Ce sistem sau flux se implementează, ce date se prelucrează, câte persoane sunt vizate, cine are acces, unde se stochează datele, cine este furnizorul.
2. Scopul și temeiul	Scopul determinat, temeiul juridic și condiția specifică pentru categoria specială de date.
3. Necesitate și proporționalitate	De ce nu se poate atinge scopul cu mai puține date; ce alternative au fost analizate; cum se aplică minimizarea și limitarea stocării.
4. Fluxul datelor	Diagrama circuitului: colectare, utilizare, stocare, partajare, arhivare, ștergere. Se indică fiecare punct de ieșire a datelor.
5. Identificarea riscurilor	Pentru fiecare risc: descrierea, sursa, probabilitatea (mică, medie, mare) și gravitatea consecinței pentru persoana vizată.
6. Măsuri de tratare	Pentru fiecare risc: măsura tehnică sau organizatorică, responsabilul, termenul și riscul rezidual după aplicare.
7. Consultări	Avizul responsabilului cu protecția datelor; consultarea structurii IT, a personalului clinic implicat și, după caz, a persoanelor vizate.
8. Concluzia	Prelucrarea poate începe / poate începe cu măsuri suplimentare / necesită consultarea prealabilă a autorității de supraveghere.
9. Monitorizare	Cine verifică aplicarea măsurilor, la ce interval și când se reevaluează.

Tabelul de risc — model de completare

Riscul identificat	Probabilitate	Gravitate	Măsura de tratare	Risc rezidual
Acces nejustificat la dosarele pacienților cu notorietate	Medie	Mare	Marcaj special, alertă la fiecare accesare, audit lunar dedicat	Mic
Export voluminos de date de către un utilizator	Medie	Mare	Limitarea implicită a exporturilor, alertă la depășirea pragului, aprobare prealabilă	Mic
Acces al furnizorului la mediul de producție	Mare	Mare	Cont nominal, aprobare per intervenție, interval limitat, înregistrarea sesiunii	Mediu

Când se consultă autoritatea de supraveghere

Atunci când, după aplicarea tuturor măsurilor rezonabile, riscul rezidual rămâne ridicat. Consultarea prealabilă este obligatorie și se realizează înainte de începerea prelucrării.

Formularul F-12

NOTIFICAREA INCIDENTULUI ȘI REGISTRUL INCIDENTELOR

Fișa de notificare, arborele de decizie și registrul. Se completează pentru fiecare incident, notificat sau nu.

Primele trei acțiuni, în ordine

1. Anunță imediat responsabilul cu protecția datelor sau superiorul ierarhic — nu aștepta să se lămurească situația.
2. Nu șterge nimic: mesajele, jurnalele și dispozitivele sunt probe.
3. Limitează efectele: blochează contul, schimbă parola, retrage documentul.

Partea I — Fișa de notificare a incidentului

Instituția medico-sanitară	[denumirea completă]
Sediul	[adresa]
Responsabilul cu protecția datelor	[nume, telefon, e-mail]

Nr. de înregistrare al incidentului	
Data și ora producerii (dacă se cunosc)	
Data și ora detectării	
Persoana care a sesizat	
Descrierea incidentului	
Natura încălcării	☐ confidențialitate ☐ integritate ☐ disponibilitate
Cauza	☐ eroare umană ☐ defecțiune tehnică ☐ atac informatic ☐ pierdere/furt ☐ altă cauză
Categoriile de date afectate	
Numărul aproximativ de persoane vizate	
Consecințe probabile pentru persoanele vizate	
Măsuri de limitare deja adoptate	
Nivelul de risc evaluat	☐ scăzut ☐ mediu ☐ ridicat
Notificare către CNPDCP	☐ Da — data și ora: _____ ☐ Nu — motivarea: _____
Informarea persoanelor vizate	☐ Da — modalitatea: _____ ☐ Nu — motivarea: _____
Măsuri preventive stabilite	

Responsabilul cu protecția datelor	Conducătorul instituției
<i>(nume, prenume, semnătura)</i>	<i>(nume, prenume, semnătura)</i>

Partea a II-a — Arborele de decizie privind notificarea

Pas	Întrebare	Consecință
1	Sunt implicate date cu caracter personal?	Nu → nu este incident în sensul legii; se tratează ca incident IT. Da → pasul 2.
2	Datele au fost distruse, pierdute, alterate, divulgate ori accesate fără drept?	Nu → nu este încălcare. Da → pasul 3.
3	Este probabil ca incidentul să genereze un risc pentru drepturile persoanelor vizate?	Nu → nu se notifică, dar se consemnează în registru, cu motivarea. Da → pasul 4.
4	Notificare la CNPDCP	Fără întârziere nejustificată și, dacă este posibil, în cel mult 72 de ore de la luarea la cunoștință. Depășirea termenului se motivează în notificare.
5	Riscul pentru persoanele vizate este ridicat?	Nu → nu se informează individual persoanele. Da → pasul 6.
6	Informarea persoanelor vizate	Fără întârziere nejustificată, în limbaj clar: ce s-a întâmplat, ce consecințe sunt posibile, ce măsuri au fost luate, ce pot face persoanele.

Datele de sănătate sunt categorie specială: în domeniul medical, un incident care le implică se prezumă, de regulă, ca generând risc. Decizia de a nu notifica se motivează în scris și se păstrează.

Partea a III-a — Registrul incidentelor de securitate

Se consemnează toate incidentele, indiferent dacă au fost sau nu notificate autorității. Se păstrează cinci ani.

Nr.	Data	Descrierea	Date afectate	Nivel de risc	Notificat	Măsuri

Formularul F-13

FIȘĂ DE ACCES ÎN REGIM DE URGENȚĂ

Se completează în cel mult 24 de ore de la fiecare acces de tip „break-the-glass”.

Când este permis accesul în regim de urgență

Atunci când starea pacientului impune consultarea imediată a datelor, iar relația clinică nu este încă înregistrată în sistem: pacient inconștient, urgență majoră, preluare în afara circuitului obișnuit. Salvarea vieții primează întotdeauna — justificarea se completează imediat după, nu înainte.

Instituția medico-sanitară	[denumirea completă]
Sediul	[adresa]
Responsabilul cu protecția datelor	[nume, telefon, e-mail]

Utilizatorul care a accesat	
Funcția și subdiviziunea	
Data și ora accesului	
Sistemul accesat	☐ SIA AMP ☐ SIA AMS ☐ eRețeta ☐ PCCM ☐ altul: _____
Pacientul accesat (nume, IDNP)	
Motivul accesului în regim de urgență	
Datele consultate	
Au fost efectuate modificări?	☐ Nu ☐ Da — se descriu: _____
Au fost efectuate exporturi sau tipăriri?	☐ Nu ☐ Da — se descriu: _____
Medicul de gardă / superiorul care confirmă	

Utilizatorul _____ (nume, prenume, semnătura)	Medicul de gardă / superiorul _____ (nume, prenume, semnătura)
---	--

Verificarea ulterioară — se completează de responsabilul cu protecția datelor

Data verificării	
Accesul a fost justificat?	☐ Da ☐ Nu ☐ Parțial
Volumul datelor consultate a fost proporțional?	☐ Da ☐ Nu
Concluzia	
Măsurile dispuse	

Semnătura responsabilului cu protecția datelor: _____ Data: ____ / ____ / ____

Regulă de sistem

Fiecare acces în regim de urgență generează automat o alertă către responsabilul cu protecția datelor și către structura IT. Verificarea ulterioară este obligatorie pentru fiecare eveniment, nu prin sondaj.

Formularul F-14

MATRICEA DE ACCES PE ROLURI

Stă la baza configurării drepturilor în sistemele informaționale. Se revizuieste semestrial și la fiecare schimbare de atribuții.

Legendă: C = citire · S = scriere · E = export · A = administrare · — = fără acces. Accesul la documentația unui pacient presupune, suplimentar, existența unei relații clinice documentate.

Rol	Dosar clinic	Rezultate laborator	Imagistică	Date administrative	Jurnale de acces	Export de date
Medic curant	C, S	C	C	C	—	E, cu justificare
Medic consultant	C (pe episod)	C	C	—	—	—
Medic de gardă	C, S (pe tură)	C	C	C	—	—
Asistent medical	C, S (limitat)	C	—	C	—	—
Registrator	—	—	—	C, S	—	—
Laborant	— (doar comanda)	C, S	—	—	—	—
Radiolog / tehnician imagistică	— (doar comanda)	—	C, S	—	—	—
Farmacist	— (doar prescripția)	—	—	C	—	—
Statistician / raportări	— (date pseudonimizate)	—	—	C	—	E, agregat
Student / rezident	C sub supraveghere	C sub supraveghere	C sub supraveghere	—	—	—
Administrator de sistem	— (fără conținut clinic)	—	—	—	C	A
Responsabil cu protecția datelor	— (fără conținut clinic)	—	—	C	C	E, pentru audit
Conducerea instituției	—	—	—	C	C, prin raport	—

Reguli de administrare a drepturilor

- Drepturile se acordă pe rol, nu pe persoană, iar persoana se atribuie unui rol.
- Orice abatere de la matrice se aprobă în scris de conducere, cu indicarea motivului și a termenului.

- Drepturile se revocă în aceeași zi la încetarea raporturilor de muncă sau la schimbarea atribuțiilor.
- Conturile inactive mai mult de 60 de zile se dezactivează automat.
- Revizuirea completă a drepturilor se efectuează semestrial și se consemnează într-un raport prezentat conducerii.

Întocmit: structura IT și DPO	Aprobat: conducătorul instituției
_____ Data: ____ / ____ / _____	_____ Data: ____ / ____ / _____

Formularul F-15

GRILĂ DE AUTOEVALUARE A CONFORMITĂȚII

Se completează anual de responsabilul cu protecția datelor și se prezintă conducerii instituției.

Pentru fiecare element se acordă un nivel de maturitate de la 0 la 3. Punctajul maxim este de 54 de puncte.

Nivel	0 — inexistent	1 — inițial	2 — implementat	3 — matur
Descriere	Elementul nu există.	Există parțial sau informal, fără document aprobat.	Există, este aprobat și se aplică.	Se aplică, se verifică periodic și se îmbunătățește pe baza constatărilor.

Nr.	Element de verificat	Dovada cerută	Responsabil	Termen	Nivel
1	Responsabil cu protecția datelor desemnat și notificat	Ordin de desemnare, fișa postului	Conducere		
2	Registrul evidențelor întocmit și actualizat	Registrul aprobat, data ultimei revizuirii	DPO		
3	Note de informare puse la dispoziție și afișate	Exemplar, fotografia afișajului	DPO / Recepție		
4	Formulare de consimțământ pentru prelucrările care îl necesită	Formularele aprobate	DPO / Juridic		
5	Contracte de prelucrare cu toți furnizorii	Lista furnizorilor și contractele	DPO / Achiziții		
6	Procedură de soluționare a cererilor persoanelor vizate	Procedura aprobată, registrul cererilor	DPO		
7	Procedură de gestionare a incidentelor	Procedura aprobată, registrul incidentelor	DPO / IT		
8	Evaluări de impact pentru prelucrările cu risc ridicat	Rapoartele de evaluare	DPO		
9	Program de instruire și evidența instruirilor	Planul de instruire, registrul instruirilor	RU / DPO		
10	Măsuri tehnice de securitate implementate	Politica de securitate, raport de configurare	IT		
11	Nomenclatorul dosarelor aprobat, cu termene de păstrare	Nomenclatorul aprobat	Arhivă / DPO		

Nr.	Element de verificat	Dovada cerută	Responsabil	Termen	Nivel
12	Videosupraveghere: decizie, informare, registrul vizionărilor	Decizia, pictogramele, registrul	Administrativ / DPO		
13	Angajamente de confidențialitate semnate de tot personalul	Dosarul angajamentelor	Resurse umane		
14	Procedură de răspuns la solicitările terților	Procedura aprobată, formularele de eliberare	Juridic / DPO		
15	Jurnalizarea accesărilor activată și audit periodic	Raportul de audit al accesărilor	IT / DPO		
16	Procedură de acces în regim de urgență, cu verificare ulterioară	Procedura, fișele completate	IT / DPO		
17	Canal instituțional securizat de comunicare medicală	Documentația soluției, politica internă	IT / Conducere		
18	Plan de implementare aprobat, cu responsabili și termene	Planul aprobat, raportul de stadiu	Conducere		

Punctaj total	Interpretare	Acțiune
0 – 18	Conformitate incipientă	Se aplică planul de implementare 30/60/90 de zile (formularul F-16), începând cu elementele 1, 2, 5 și 13.
19 – 36	Conformitate parțială	Se prioritizează elementele cu nivel 0 și 1; se stabilesc termene ferme și responsabili nominali.
37 – 47	Conformitate bună	Se consolidează verificarea periodică: audit al accesărilor, revizuirea drepturilor, testarea copiilor de rezervă.
48 – 54	Conformitate matură	Se menține ritmul de verificare și se documentează îmbunătățirile pentru controlul următor.

Punctaj obținut: _____ / 54 Data evaluării: ____ / ____ / ____ Semnătura DPO: _____

Formularul F-16

PLAN DE IMPLEMENTARE 30 / 60 / 90 DE ZILE

Traseu pentru instituțiile care încep implementarea. Se aprobă de conducere și se raportează lunar.

Instituția medico-sanitară	[denumirea completă]
Sediul	[adresa]
Responsabilul cu protecția datelor	[nume, telefon, e-mail]
Responsabil de implementare	[nume, funcție]
Data începerii	___ / ___ / ____

Etapa I — Primele 30 de zile: fundația

Nr.	Acțiune	Responsabil	Livrabil
1	Desemnarea responsabilului cu protecția datelor și stabilirea atribuțiilor	Conducere	Ordin de desemnare, fișa postului
2	Inventarierea activităților de prelucrare, pe subdiviziuni	DPO	Inventar preliminar
3	Identificarea tuturor furnizorilor cu acces la date	DPO / Achiziții	Lista furnizorilor
4	Afișarea notei de informare a pacientului și a materialelor de afișare	DPO / Administrativ	Materiale afișate, fotografii
5	Comunicarea internă privind interdicția canalelor neaprobate	Conducere	Notă internă, confirmare de luare la cunoștință

Etapa a II-a — Zilele 31–60: documentele

Nr.	Acțiune	Responsabil	Livrabil
6	Întocmirea registrului evidențelor activităților de prelucrare	DPO	Registru aprobat
7	Aprobarea nomenclatorului dosarelor, cu termene de păstrare	Arhivă / DPO	Nomenclator aprobat
8	Încheierea contractelor de prelucrare cu toți furnizorii identificați	Juridic / Achiziții	Contracte semnate
9	Aprobarea procedurii de soluționare a cererilor persoanelor vizate	DPO	Procedură, registrul cererilor
10	Aprobarea procedurii de gestionare a incidentelor	DPO / IT	Procedură, registrul incidentelor
11	Semnarea angajamentelor de confidențialitate de întregul personal	Resurse umane	Dosarul angajamentelor

Etapa a III-a — Zilele 61–90: aplicarea și verificarea

Nr.	Acțiune	Responsabil	Livrabil
12	Revizuirea drepturilor de acces pe roluri, conform matricei	IT / DPO	Matricea aplicată, raport de revizuire

Nr.	Acțiune	Responsabil	Livrabil
13	Activarea jurnalizării și primul audit al accesărilor	IT / DPO	Raport de audit
14	Instruirea întregului personal și susținerea testului de evaluare	RU / DPO	Registrul instruirilor, rezultatele testului
15	Evaluări de impact pentru prelucrările cu risc ridicat	DPO	Rapoarte de evaluare
16	Reglementarea videosupravegherii: decizie, informare, registru	Administrativ / DPO	Decizia și registrul
17	Autoevaluarea conformității și prezentarea rezultatului conducerii	DPO	Grila completată, raport

Ordinea contează

Elementele 1, 2, 6 și 8 sunt fundația: fără responsabil desemnat, fără inventar, fără registru și fără contracte cu furnizorii, celelalte măsuri nu pot fi demonstrate în cazul unui control. Instituțiile mici pot comprima etapele, dar nu pot schimba ordinea.

Întocmit	Aprobat: conducătorul instituției
_____ Data: ____ / ____ / ____	_____ Data: ____ / ____ / ____

Formularul F-17

REGISTRUL INSTRUIRILOR ȘI TEST DE EVALUARE

Instruirea este obligatorie la încadrare și cel puțin anual. Evidența constituie element de demonstrare a conformității.

Partea I — Registrul instruirilor

Nr.	Nume, prenume	Funcția	Data instruirii	Rezultat test	Semnătura

Instruirea a fost susținută de: _____ Data: ____ / ____ / ____

Partea a II-a — Test de evaluare

Nume, prenume: _____ Funcția: _____ Data: _____
 ____ / ____ / ____

Se bifează un singur răspuns corect pentru fiecare întrebare. Prag de promovare: 15 răspunsuri corecte din 20.

1. Un coleg vă roagă să verificați rezultatul analizelor soției lui, care este pacienta instituției. Ce faceți?

☐	a) Verific, pentru că este colegul meu
☐	b) Refuz și îl îndrum către procedura oficială de acces
☐	c) Verific, dar nu îi spun rezultatul
☐	d) Verific numai dacă are acordul verbal al soției

2. Este necesar consimțământul pacientului pentru prelucrarea datelor în scopul tratamentului?

☐	a) Nu, temeiul este acordarea asistenței medicale
☐	b) Da, dar numai pentru analize
☐	c) Numai pentru pacienții internați
☐	d) Da, întotdeauna

3. Un pacient cere copia dosarului său. În ce termen răspundeți?

☐	a) În termen de o lună de la înregistrarea cererii
☐	b) Nu există termen
☐	c) În 3 zile
☐	d) În 10 zile

4. O rudă cere documentația medicală a unui pacient adult și conștient. Ce faceți?

☐	a) Îl eliberez după verificarea buletinului rudei
☐	b) Îl eliberez, este rudă de gradul I
☐	c) Îl eliberez numai cu acordul scris al pacientului sau cu procură
☐	d) Îl eliberez dacă pacientul este internat

5. În cât timp se notifică autoritățile de supraveghere un incident cu risc?

☐	a) În 24 de ore
☐	b) Fără întârziere și, dacă este posibil, în cel mult 72 de ore
☐	c) În 7 zile

☐	d) Numai dacă au fost afectate peste 100 de persoane
--------------------------	--

6. Puteți trimite rezultatul unei analize pe o aplicație publică de mesagerie, la cererea pacientului?

☐	a) Da, dacă șterg mesajul după
☐	b) Nu; se folosesc canalele instituționale
☐	c) Da, dacă trimit doar o fotografie
☐	d) Da, dacă pacientul cere expres

7. Ce faceți când părăsiți postul de lucru pentru câteva minute?

☐	a) Închid doar monitorul
☐	b) Îmi las contul deschis pentru colegi
☐	c) Las calculatorul deschis, revin repede
☐	d) Blochez sesiunea

8. O persoană sună și întreabă dacă un pacient este internat. Ce răspundeți?

☐	a) Confirm doar numărul salonului
☐	b) Confirm, este o informație banală
☐	c) Nu confirm și nu infirm; aplic procedura de verificare
☐	d) Confirm dacă apelantul spune că este rudă

9. Fotografați o leziune pentru documentația pacientului. Cu ce echipament?

☐	a) Cu telefonul personal, apoi transfer imaginea
☐	b) Cu echipament instituțional, stocare în sistemul medical
☐	c) Cu telefonul personal, dacă șterg imediat
☐	d) Cu orice echipament, dacă pacientul acceptă

10. Ce înseamnă că fiecare accesare este jurnalizată?

☐	a) Că se înregistrează cine, ce, când și ce operațiune, și poate fi auditat
☐	b) Că se înregistrează doar exporturile
☐	c) Că se șterge după 24 de ore
☐	d) Că se salvează doar erorile

11. Un pacient cere ștergerea unui diagnostic corect din documentația medicală. Ce faceți?

☐	a) Îl șterg numai din sistemul electronic
☐	b) Refuz fără să răspund în scris
☐	c) Îl șterg, este dreptul lui

☐	d) Analizez cererea cu DPO și răspund motivat; ștergerea este limitată de arhivare
--------------------------	--

12. Ați trimis din greșeală un document cu date de pacient la o adresă greșită. Ce faceți?

☐	a) Trimit un mesaj de retragere și închid subiectul
☐	b) Nimic, a fost o greșeală mică
☐	c) Anunț imediat DPO și cer destinatarului ștergerea
☐	d) Aștept să văd dacă răspunde cineva

13. Cui i se comunică rezultatul examenului medical periodic al angajatului?

☐	a) Angajatorului, integral
☐	b) Angajatorului, numai concluzia de aptitudine
☐	c) Colegilor din subdiviziune
☐	d) Nimănui, nici angajatului

14. Un procuror solicită telefonic date despre un pacient. Ce faceți?

☐	a) Solicit cererea în scris, cu indicarea temeiului
☐	b) Le comunic doar parțial
☐	c) Le comunic dacă îmi trimite un mesaj
☐	d) Le comunic, este procuror

15. Ce se întâmplă cu o fișă medicală care nu mai este necesară?

☐	a) Se lasă în arhivă la nesfârșit
☐	b) Se rupe în două și se aruncă
☐	c) Se aruncă la coșul de birou
☐	d) Se distruge securizat, prin tocare

16. Accesul în regim de urgență („break-the-glass”) este permis:

☐	a) Niciodată
☐	b) Oricând, pentru comoditate
☐	c) Când starea pacientului o impune, cu justificare completată ulterior
☐	d) Numai cu aprobare scrisă prealabilă

17. Cât se păstrează, de regulă, înregistrările de videosupraveghere?

☐	a) Un an
☐	b) Cel mult 30 de zile
☐	c) Cinci ani

☐	d) Nelimitat
--------------------------	--------------

18. Ce date primește angajatorul dintr-un certificat de concediu medical?

☐	a) Perioada și codul de indemnizație, fără diagnostic
☐	b) Toate investigațiile efectuate
☐	c) Numele medicului curant și diagnosticul
☐	d) Diagnosticul complet

19. Anonimizarea unui set de date înseamnă:

☐	a) Ștergerea adresei
☐	b) Criptarea fișierului
☐	c) Înlocuirea numelui cu un cod păstrat separat
☐	d) Eliminarea ireversibilă a posibilității de identificare

20. Când începe obligația de confidențialitate a personalului tehnic?

☐	a) Doar dacă semnează un contract separat
☐	b) Nu li se aplică
☐	c) Din momentul în care pot accesa date de sănătate, și continuă după încetarea contractului
☐	d) Doar în timpul programului de lucru

Grila de răspunsuri corecte

1-b · 2-a · 3-a · 4-c · 5-b · 6-b · 7-d · 8-c · 9-b · 10-a · 11-d · 12-c · 13-b · 14-a · 15-d · 16-c ·
17-b · 18-a · 19-d · 20-c

Grila se detașează înainte de distribuirea testului.

VIDEOSUPRAVEGHERE: DECIZIE, INFORMARE, REGISTRU

Se completează înainte de punerea în funcțiune a sistemului de videosupraveghere.

Partea I — Decizia de instalare

Instituția medico-sanitară	[denumirea completă]
Sediul	[adresa]
Responsabilul cu protecția datelor	[nume, telefon, e-mail]

Decizia nr. _____ din ____ / ____ / _____

Scopul supravegherii	Securitatea persoanelor și a bunurilor, controlul accesului în zone cu regim restricționat, prevenirea incidentelor
Zonele acoperite	
Zonele expres excluse	Saloane, cabinete de consultație și tratament, vestiare, grupuri sanitare, spații de odihnă ale personalului
Numărul și tipul camerelor	
Înregistrare audio	☐ Nu (regula) ☐ Da — temeiul distinct și evaluarea de impact: _____
Termenul de păstrare	Cel mult 30 de zile
Persoanele autorizate să vizioneze	
Locul de amplasare a echipamentelor de stocare	
Măsuri de securitate	Acces nominal, cameră încuiată, jurnalizarea vizionărilor, ștergere automată la expirarea termenului
Avizul responsabilului cu protecția datelor	

Conducătorul instituției _____ (nume, prenume, semnătura)	Responsabilul cu protecția datelor _____ (nume, prenume, semnătura)
--	--

Partea a II-a — Notă de informare privind videosupravegherea

Se afișează la fiecare intrare în zona supravegheată, alături de pictograma cu camera de luat vederi.

ZONĂ SUPRAVEGHEATĂ VIDEO

Operator: [denumirea instituției], [adresa]

Scopul: securitatea persoanelor și a bunurilor

Durata de păstrare: cel mult 30 de zile

Responsabilul cu protecția datelor: [nume, telefon, e-mail]

Aveți dreptul de acces la imaginile care vă privesc, de restricționare și de opoziție, precum și dreptul de a sesiza CNPDCP (www.datepersonale.md). Nota de informare completă este disponibilă la recepție și pe pagina web a instituției.

Nota de informare completă — elemente obligatorii

- identitatea și datele de contact ale operatorului și ale responsabilului cu protecția datelor;
- scopurile și temeiul prelucrării;
- zonele supravegheate și cele excluse;
- durata de păstrare și modalitatea de ștergere;
- destinatarii imaginilor și condițiile de transmitere către autorități;
- drepturile persoanelor vizate și modul de exercitare;
- dreptul de a sesiza autoritatea de supraveghere.

Partea a III-a — Registrul vizionărilor

Fiecare vizionare a înregistrărilor se consemnează, indiferent de motiv și de durată.

Nr.	Data	Persoana care a vizionat	Motivul	Intervalul vizionat	Semnătura

Interdicții

Camerele ascunse, înregistrarea audio și recunoașterea facială necesită un temei distinct și o evaluare de impact prealabilă. Videosupravegherea nu se utilizează pentru monitorizarea activității sau a performanței personalului. Imaginile nu se difuzează și nu se publică.

Formularul F-19

PROCES-VERBAL DE DISTRUGERE SECURIZATĂ

Se întocmește la fiecare eliminare de documente sau suporturi care conțin date cu caracter personal.

Instituția medico-sanitară	[denumirea completă]
Sediul	[adresa]
Responsabilul cu protecția datelor	[nume, telefon, e-mail]

Proces-verbal nr. _____ din ____ / ____ / _____

Comisia constituită prin [ordinul nr. _____ din ____ / ____ / _____], formată din:

Nr.	Nume, prenume	Funcția	Semnătura
1			
2			
3			

a procedat la distrugerea securizată a următoarelor documente și suporturi, ale căror termene de păstrare au expirat potrivit nomenclatorului dosarelor aprobat al instituției:

I. Documente pe suport de hârtie

Nr.	Categoria documentelor	Perioada	Cantitate	Termen expirat la
1				
2				
3				
4				
5				
6				

II. Suporturi electronice

Nr.	Tipul suportului	Serie / identificator	Metoda de distrugere
1			
2			
3			
4			

III. Metoda utilizată

☐	Tocare mecanică, cu tăiere încrucișată (nivel de securitate P-4 sau superior)
☐	Incinerare
☐	Predare către un prestator autorizat, în baza contractului nr. _____ din ____ / ____ / _____
☐	Ștergere securizată prin suprascriere, urmată de distrugerea fizică a suportului
☐	Distrugerea fizică a suportului electronic

Distrugerea s-a efectuat în data de ____ / ____ / _____, la sediul instituției / la sediul prestatorului, în prezența membrilor comisiei. Din documentele și suporturile distruse nu mai poate fi recuperată nicio informație.

Președintele comisiei	Responsabilul cu protecția datelor
_____	_____
<i>(nume, prenume, semnătura)</i>	<i>(nume, prenume, semnătura)</i>

De reținut

Se distrug securizat și elementele mărunte: etichetele de la probe, brățările de identificare, ciornele, listele de programări, benzile de la aparate. Nimic care conține nume, IDNP sau diagnostic nu ajunge la deșeurile obișnuite. Prezentul proces-verbal se păstrează cinci ani.

CELE ȘASE REGULI DE AUR

Protecția datelor pacientului · ce se aplică în fiecare zi, de fiecare dintre noi

1

Contul meu, parola mea

Nu împrumut contul nimănui și nu îl folosesc pe al altcuiva. Fiecare acțiune rămâne pe numele meu.

2

Blochez ecranul când plec

Chiar și pentru un minut. Tasta Windows + L.

3

Doar pacienții mei

Deschid exclusiv documentația pacienților aflați în îngrijirea mea. Fiecare accesare este înregistrată.

4

Numai canale instituționale

Rezultatele și imaginile circulă prin sistemul instituției, niciodată prin aplicații personale de mesagerie.

5

Hârtia la tocător

Fișe, etichete, brățări, ciorne — nimic cu nume sau diagnostic nu ajunge la coșul obișnuit.

6

Anunț imediat orice incident

Mesaj trimis greșit, dispozitiv pierdut, document rătăcit: primele ore contează cel mai mult.

Responsabilul cu protecția datelor din instituție:

Nume: _____

Telefon: _____

E-mail: _____

NU DESCHIDE DOSARUL UNEI PERSOANE CUNOSCUTE

Nici al unei rude. Nici al unui coleg. Nici „doar ca să văd dacă e bine”.

Accesarea documentației în afara implicării în îngrijire este o abatere — chiar dacă nu spui nimănui nimic, chiar dacă persoana ți-ar fi dat acordul verbal, chiar dacă ai făcut-o din grijă.

1

Fiecare accesare este înregistrată

Sistemul reține cine a deschis documentația, când și ce a consultat.

2

Pacientul îți poate vedea numele

În „Istoricul accesului” la propria documentație, pacientul vede fiecare accesare.

3

Verificările se fac periodic

Auditul accesărilor este parte din activitatea curentă, nu o măsură excepțională.

4

Consecințele sunt personale

Răspunderea disciplinară se aplică persoanei care a accesat, independent de existența unui prejudiciu.

Ce faci în schimb

Îndrumi persoana interesată să depună o cerere de acces la propriile date, la registratură sau la responsabilul cu protecția datelor. Răspunsul vine în cel mult o lună, gratuit.

Responsabilul cu protecția datelor din instituție:

Nume: _____

Telefon: _____

E-mail: _____

LA TELEFON

Ce pot spune și ce nu spun niciodată

POT SPUNE

- Programul instituției și al cabinetelor.
- Modul de programare și documentele necesare.
- Informații despre propriile date, DUPĂ verificarea identității apelantului.
- Informații despre un pacient, către persoana pe care pacientul a indicat-o în scris.

NU SPUN NICIODATĂ

- Dacă o persoană este sau nu internată — nici măcar atât.
- Diagnosticul, rezultatele, tratamentul sau starea unui pacient.
- Numărul salonului sau secția în care se află cineva.
- Nimic, dacă nu am putut verifica cine sună.

Formula de refuz, cuvânt cu cuvânt

„Nu pot confirma sau infirma prin telefon nicio informație despre pacienți. Vă rog să vă adresați în scris instituției sau să solicitați informația direct de la pacient.”

Regula de aur

În caz de dubiu, nu divulg. Nimeni nu a fost sancționat pentru că a fost prudent la telefon.

Responsabilul cu protecția datelor din instituție:

Nume: _____

Telefon: _____

E-mail: _____

DATELE PACIENTULUI NU CIRCULĂ PE APLICAȚII PERSONALE

NU -> WhatsApp · Telegram · Viber · Messenger · conturi personale de e-mail

De ce este interzis

Pe aceste canale instituția pierde controlul asupra datelor: nu se știe cine mai are acces, nu există trasabilitate, nu se poate face audit și nu se poate demonstra ce s-a transmis. Un mesaj trimis greșit nu mai poate fi retras.

FOLOSEȘTE

- Mesageria internă a sistemului informațional.
- E-mailul instituțional, cu document protejat.
- Portalurile securizate ale instituției.
- Rețeaua medicală securizată, pentru imagistică.

NU FOLOSI

- Aplicații publice de mesagerie, pentru rezultate sau imagini.
- Conturi personale de e-mail.
- Fotografii ale documentelor, făcute cu telefonul personal.
- Grupuri de mesagerie cu nume și diagnostice de pacienți.

Pentru discuții organizatorice

Un grup de mesagerie poate fi folosit pentru chestiuni de organizare — ședințe, anunțuri — atâta timp cât niciun pacient nu poate fi identificat.

Responsabilul cu protecția datelor din instituție:

Nume: _____

Telefon: _____

E-mail: _____

AI GREȘIT? ANUNȚĂ ÎN PRIMA ORĂ

Un incident anunțat repede se rezolvă. Unul ascuns devine o problemă mult mai mare.

1

Anunță imediat

Responsabilul cu protecția datelor sau șeful direct. Nu aștepta să se lămurească situația singură.

2

Nu șterge nimic

Mesajele, jurnalele și dispozitivele sunt probe. Ștergerea îngreunează evaluarea și agravează situația.

3

Limitează efectele

Blochează contul, schimbă parola, cere destinatarului greșit să șteargă documentul.

4

Scrie ce s-a întâmplat

Data, ora, ce date au fost implicate, câte persoane, ce ai făcut deja.

Ce contează ca incident

Mesaj sau document trimis către destinatarul greșit · laptop, telefon sau stick pierdut ori furat · documentație pe hârtie rătăcită · cont accesat de altcineva · program malițios · orice divulgare accidentală.

Termenul legal

Instituția are cel mult 72 de ore pentru a notifica autoritatea de supraveghere. Ceasul pornește când instituția află — deci din clipa în care anunți.

Anunță incidentul aici:

Nume: _____

Telefon: _____

E-mail: _____

BIROU ORDONAT = ECRAN BLOCAT

1

Windows + L, de fiecare dată

Când te ridici de la birou, chiar și pentru un minut.

2

Ecranul nu se vede din sala de așteptare

Reorientează monitorul sau cere un filtru de confidențialitate.

3

Documentele nu rămân pe birou

La plecare, în sertar sau în dulap, sub cheie.

4

Nimic uitat pe imprimantă

Ridică documentul imediat ce l-ai tipărit.

5

Fișa se închide între doi pacienți

Înainte de a chema următorul pacient.

Responsabilul cu protecția datelor din instituție:

Nume: _____

Telefon: _____

E-mail: _____

Ghid privind protecția datelor cu caracter personal în domeniul sănătății · Ministerul Sănătății al Republicii Moldova · Ediția I, 2026

DREPTURILE DUMNEAVOASTRĂ ASUPRA DATELOR MEDICALE

Informație pentru pacienți

Datele dumneavoastră medicale sunt confidențiale. Le prelucrăm pentru a vă acorda îngrijire și pentru a respecta obligațiile legale ale instituției. Aveți următoarele drepturi:

- 1** Să știți ce date avem despre dumneavoastră și în ce scop le folosim.
- 2** Să primiți o copie a dosarului gratuit, în cel mult o lună de la cerere.
- 3** Să cereți corectarea datelor greșite sau completarea celor incomplete.
- 4** Să cereți ștergerea unor date în limitele legii — documentația medicală se arhivează obligatoriu.
- 5** Să vedeți cine v-a accesat documentația prin „Istoricul accesului” la dosarul electronic de sănătate.
- 6** Să depuneți o plângere la instituție sau la Centrul Național pentru Protecția Datelor cu Caracter Personal.

Cum procedați

Cereți formularul la registratură sau adresați-vă responsabilului cu protecția datelor. Vă răspundem în scris, gratuit, în cel mult o lună. Dacă nu putem admite cererea, vă explicăm de ce și cum puteți contesta.

Ce nu facem niciodată

Nu confirmăm nimănui prin telefon că sunteți internat. Nu comunicăm diagnosticul rudelor fără acordul dumneavoastră. Nu transmitem datele angajatorului.

Responsabilul cu protecția datelor din această instituție:

Nume: _____

Telefon: _____

Email: _____

DOCUMENTELE PE HÂRTIE

Nimic cu nume, IDNP sau diagnostic nu ajunge la coșul obișnuit

LA TOCĂTOR

- Fișe și file din documentația medicală.
- Etichete de la probe și brățări de identificare.
- Liste de programări și de internări.
- Ciorne, notițe, benzi tipărite de aparate.
- Copii tipărite din greșeală.

NICIODATĂ

- La coșul de birou.
- La deșeurile obișnuite.
- Rupte în două și aruncate.
- Lăsate în cutii, în spații accesibile.
- Refolosite ca hârtie de ciornă.

Documentele cu termen expirat

Se elimină pe bază de proces-verbal, de o comisie, potrivit nomenclatorului dosarelor aprobat al instituției. Nu se aruncă individual.

Responsabilul cu protecția datelor din instituție:

Nume: _____

Telefon: _____

E-mail: _____

ACCES ÎN REGIM DE URGENȚĂ

Salvarea vieții primează. Justificarea se scrie imediat după.

Când este permis

Când starea pacientului impune consultarea imediată a datelor, iar relația clinică nu este încă înregistrată în sistem: pacient inconștient, urgență majoră, preluare în afara circuitului obișnuit.

1

Accesează și tratează

Nu întârzia îngrijirea pentru formalități. Sistemul îți permite accesul.

2

Consultă doar ce îți trebuie

Volumul datelor consultate trebuie să fie proporțional cu urgența.

3

Completează fișa în 24 de ore

Formularul F-13: cine, când, ce pacient, de ce, ce date ai consultat.

4

Așteaptă verificarea

Fiecare acces de acest tip generează o alertă și este verificat ulterior. Este normal și nu este o suspiciune.

Ce NU este acces în regim de urgență

Comoditatea, graba obișnuită, lipsa drepturilor potrivite pentru postul tău sau curiozitatea. Dacă îți lipsesc drepturi de care ai nevoie zilnic, se solicită modificarea rolului, nu accesul de urgență.

Responsabilul cu protecția datelor din instituție:

Nume: _____

Telefon: _____

E-mail: _____

FOTOGRAFII CLINICE

Numai cu echipamentul instituției. Numai în sistemul medical.

DA

- Echipament al instituției.
- Stocare directă în sistemul medical.
- Acordul scris al pacientului, când imaginea îl poate identifica.
- Cadru limitat la zona relevantă clinic.

NU

- Telefonul personal — nici „doar temporar”.
- Galeria telefonului sau cloudul personal.
- Trimiterea pe aplicații de mesagerie.
- Publicarea pe rețele sociale, chiar anonimizată insuficient.

De ce nu ajunge să ștergi imaginea de pe telefon

Fotografiile se sincronizează automat în servicii externe de stocare în câteva secunde. Ștergerea din galerie nu le elimină de acolo, iar instituția nu mai poate demonstra ce s-a întâmplat cu ele.

Pentru prezentări și publicare

Este necesar consimțământul explicit, pe formularul din formularul F-03, plus avizul intern. Materialele se anonimizează complet.

Responsabilul cu protecția datelor din instituție:

Nume: _____

Telefon: _____

E-mail: _____

STUDENȚI ȘI REZIDENȚI

Aveți acces la informația medicală. Aveți și obligațiile care vin cu ea.

1

Numai sub supraveghere

Accesul la documentație se face în prezența și cu acordul cadrului didactic sau al medicului responsabil.

2

Numai în scop didactic

Nu deschizi documentația unei cunoștințe, al unei rude sau al unei persoane care te interesează personal.

3

Fără fotografii, fără copii

Nu fotografiezi ecrane, documente sau pacienți. Nu extragi date din sistem.

4

Fără povestit

Cazurile nu se discută în afara activității didactice și nu ajung niciodată pe rețele sociale.

5

Anonimizare completă în lucrări

Nume, IDNP, date, secție, medic curant — orice combinație poate identifica pacientul.

6

Obligația continuă după stagiul

Secretul profesional nu se încheie odată cu practica.

Fiecare accesare rămâne pe numele tău

Sistemul înregistrează cine a deschis fiecare documentație. Accesul didactic se documentează. Pacientul poate vedea accesările la propria documentație.

Coordonatorul de stagiul și responsabilul cu protecția datelor:

Nume: _____

Telefon: _____

E-mail: _____