

## INSTRUCȚIUNI

### în legătură cu prelucrarea datelor cu caracter personal privind starea de sănătate

Prezentele instrucțiuni sunt elaborate în conformitate cu prevederile art. 20 alin. (1) lit. c) al Legii privind protecția datelor cu caracter personal, în scopul ajustării operațiunilor de prelucrare a datelor cu caracter personal privind starea de sănătate, în acord cu principiile generale de protecție a datelor cu caracter personal.

Centrul Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova (CNPDCP), în exercitarea jurisdicției sale de garant al respectării protecției datelor cu caracter personal și a pârghiilor de competență reglementate prin Legea privind protecția datelor cu caracter personal, având drept premisă:

- *considerentul umanist* că operațiunile de prelucrare a datelor cu caracter personal sunt în serviciul omului și drepturilor sale;
- *principiile generale* pentru prelucrarea datelor cu caracter personal consacrate în Convenția pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal nr. 108, deschisă spre semnare la 28 ianuarie 1981 (Convenția nr. 108) și de obligația Republicii Moldova de a asigura respectarea dreptului la inviolabilitatea vieții private și extensiunea acestuia – dreptul la protecția datelor cu caracter personal, coroborat cu alte obligații pozitive ale Statului, inclusiv cea de a respecta și ocroti viața intimă, familială și privată;
- *prelucrarea automatizată și neautomatizată* a datelor cu caracter personal privind starea de sănătate, a devenit una pregnantă nu doar la acordarea asistenței medicale, cercetări științifice în domeniul sănătății, gestionarea spitalelor și a sănătății publice, însă și în afara sectorului medical;
- *importanța calității, integrității și disponibilității* datelor cu caracter personal privind starea de sănătate care garantează sănătatea subiectului de date și a apropiaților săi;
- *progresul științelor medicale* depinde în mare măsură de disponibilitatea datelor cu caracter personal privind starea de sănătate a persoanelor;
- *necesitatea unei reglementări însoțite de garanții* a procesului de colectare și prelucrare a datelor cu caracter personal privind starea de sănătate, în scopul asigurării confidențialității și securității datelor cu caracter personal privind starea de sănătate;
- *constatările CNPDCP* în procesul examinării unei serii de plângeri cu referire la încălcarea principiilor de protecție a datelor cu caracter personal de către instituțiile medico-sanitare, precum și în procesul implementării de către unele instituții medicale, a sistemelor informaționale de prelucrare automatizată a datelor cu caracter personal care vizează personalul și pacienții acestora, pentru a asigura colectarea, transmiterea, centralizarea, stocarea, prelucrarea și vizualizarea informațiilor, în scopul soluționării problemelor complexe de examinare a pacienților și de dirijare a serviciilor de sănătate;

elaborează prezentele instrucțiuni în scopul alinierii operațiunilor de prelucrare a datelor cu caracter personal, efectuate de către operatorii de date cu caracter personal, în conformitate cu principiile de protecție a datelor cu caracter personal.

\* Prin prisma Legii nr. 274 din 07.11.2013 privind formularea unor declarații ale Republicii Moldova la Convenția pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, Republica Moldova și-a asumat obligația de a aplica prevederile Convenției 108 în aceeași măsură fișierelor de date cu caracter personal care nu fac obiectul prelucrării automatizate.

## CAPITOLUL I

### DISPOZIȚII GENERALE

#### 1. Scopul și fundamentarea necesității

Prelucrarea datelor cu caracter personal privind starea de sănătate trebuie realizată în siguranță și cu asigurarea măsurilor de securitate adaptate la riscurile pentru drepturile și libertățile fundamentale ce trebuie definite în acest sens pentru a se asigura că toate părțile interesate respectă standarde ridicate care garantează legalitatea prelucrării, securitatea și confidențialitatea datelor medicale prelucrate.

Toți subiecții de date cu caracter personal/pacienții au dreptul la confidențialitatea datelor cu caracter personal privind starea de sănătate și pot pretinde în mod rezonabil ca protecția și confidențialitatea propriilor date cu caracter personal să fie supuse unor reguli riguroase de prelucrare.

Prezentele Instrucțiuni sunt elaborate în scopul configurării unui set de cerințe pentru prelucrarea datelor cu caracter personal privind starea de sănătate, recomandate a fi respectate de către operatorii de date cu caracter personal, fiind opozabile atât față de operatorii din sectorul public, cât și față de operatorii din sectorul privat.

Instrucțiunile în cauză nu reprezintă un set de reguli exhaustive, ci urmează a fi abordate ca fiind linii directorii menite să înlesnească procesul de prelucrare a datelor cu caracter personal privind starea de sănătate a subiecților de date, prin prisma unor garanții adecvate de protecție a datelor cu caracter personal privind starea de sănătate.

*Per ansamblu*, obiectivul prezentelor Instrucțiuni este de a consolida protecția dreptului la inviolabilitatea vieții private, proclamat și recunoscut prin articolul 8 din Convenția pentru apărarea drepturilor omului și a libertăților fundamentale<sup>2</sup> și art. 27 al Constituției Republicii Moldova.

#### 2. Noțiuni și considerații generale relevante în materie de prelucrare a datelor cu caracter personal privind starea de sănătate

În sensul prezentelor Instrucțiuni, prezintă relevanță următoarele noțiuni:

**date cu caracter personal** – orice informație referitoare la o persoană fizică identificată sau identificabilă (subiect al datelor cu caracter personal). Persoana identificabilă este persoana care poate fi identificată, direct sau indirect, prin referire la un număr de identificare sau la unul ori mai multe elemente specifice identității sale fizice, fiziologice, psihice, economice, culturale sau sociale. **De exemplu:** numele, prenumele, sexul, data nașterii, grupa sanguină, boli cronice, faptul internării/spitalizării, etc.

**categorii speciale de date cu caracter personal** – datele care dezvăluie originea rasială sau etnică a persoanei, convingerile ei politice, religioase sau filozofice, apartenența socială, datele privind starea de sănătate, precum și cele referitoare la condamnările penale, măsurile procesuale de constrângere sau sancțiunile contravenționale.

**prelucrarea datelor cu caracter personal** – orice operațiune sau serie de operațiuni care se efectuează asupra datelor cu caracter personal prin mijloace automatizate sau neautomatizate, cum ar fi: colectarea, înregistrarea, organizarea, stocarea, păstrarea, restabilirea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ștergerea sau distrugerea. **De exemplu:** colectarea, stocarea, transmiterea, vizualizarea informațiilor despre pacienți, constituie operațiuni de prelucrare a datelor cu caracter personal.

**operator** – persoana fizică sau persoana juridică de drept public sau de drept privat, inclusiv autoritatea publică, orice altă instituție ori organizație care, în mod individual sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal prevăzute în mod expres de legislația în vigoare. **De exemplu:** instituțiile medico-sanitare sînt considerate operatori de date cu

<sup>2</sup> Adoptată la Roma la 04 noiembrie 1950 de către statele membre ale Consiliului Europei; intrată în vigoare la 03 septembrie 1953; ratificată prin Hotărârea de Parlament nr.1298-XIII din 24 iulie 1997 și în vigoare pentru Republica Moldova din 12 septembrie 1997.

caracter personal în partea ce ține de prelucrarea manuală sau automatizată a datelor cu caracter personal în sisteme de evidență menite să asigure programarea vizitelor pacienților la medic.

**persoană împuternicită de către operator** - persoana fizică sau persoana juridică de drept public ori de drept privat, inclusiv autoritatea publică și subdiviziunile ei teritoriale, care prelucrează date cu caracter personal în numele și pe seama operatorului, pe baza instrucțiunilor primite de la operator. **De exemplu:** dacă sistemele informaționale sau camerele CCTV instalate în instituțiile medico-sanitare sînt gestionate tehnic în conformitate cu instrucțiunile instituției medico-sanitare de către un furnizor de servicii în contextul de externalizare a resurselor (outsourcing), acel furnizor va fi considerat drept persoană împuternicită de către operator.

**destinatar** - orice persoană fizică sau persoană juridică de drept public ori de drept privat, inclusiv autoritatea publică și subdiviziunile ei teritoriale, căreia îi sînt dezvăluite date cu caracter personal, indiferent dacă este sau nu terț.

**sistem de evidență a datelor cu caracter personal** - orice serie structurată de date cu caracter personal accesibile conform unor criterii specifice, fie că este centralizată, descentralizată ori repartizată după criterii funcționale sau geografice. În calitate de sistem de evidență a datelor cu caracter personal se constituie, inclusiv, dar nu se limitează la, bazele de date, sistemele informaționale și informatice în care sînt stocate și preluate automatizat sau manual date cu caracter personal. **De exemplu:** evidența/sistematizarea în ordine alfabetică a datelor pacienților tratați în baza polițelor de asigurare medicală, ținută manual sau electronic, în cadrul unor registre. Se consideră sistem de evidență a datelor cu caracter personal: cartelele medicale; listele cu programările la medic, etc.

**depersonalizarea datelor** - modificarea datelor cu caracter personal astfel încît detaliile privind circumstanțele personale sau materiale să nu mai permită atribuirea acestora unei persoane fizice identificate sau identificabile ori să permită atribuirea doar în condițiile unei investigații care necesită cheltuieli disproporționate de timp, mijloace și forță de muncă.

Reieșind din definiția „*datelor cu caracter personal*” și „*categoriilor speciale de date*” reglementate de Legea privind protecția datelor cu caracter personal, precum și din prevederile art. 6 al aceluiași act legislativ, care stipulează expres că „*Prelucrarea categoriilor speciale de date cu caracter personal este interzisă, cu excepția anumitor cazuri...*”, prelucrarea datelor cu caracter personal privind starea de sănătate a unei persoane, reprezintă o prelucrare sensibilă, aptă să genereze riscuri considerabile în adresa drepturilor subiecților de date, pe cale de consecință, solicită și o protecție specială.

Simpla menționare a faptului, că o anumită persoană s-a rănit la picior și se află în concediu din considerente medicale, constituie date cu caracter personal privind starea de sănătate, în sensul art. 3 din Legea privind protecția datelor cu caracter personal<sup>3</sup>. Această definiție se aplică și datelor cu caracter personal când acestea au o legătură clară și apropiată cu descrierea stării de sănătate a unei persoane: datele privind consumul de medicamente, alcool sau droguri, precum și datele genetice, reprezintă, fără îndoială, date cu caracter personal privind starea de sănătate, în special dacă sunt sistematizate și incluse într-un dosar medical.

De asemenea, orice alte date - de exemplu, datele administrative (numărul poliței de asigurare medicală, faptul internării în spital, etc.), aflate în documentația medicală a pacientului vor fi considerate ca date cu caracter personal privind starea de sănătate a subiectului.

În consecință, toate datele conținute în documentația medicală, în dosarul pacientului și în sistemele informaționale ce prelucrează aceste date, trebuie considerate a fi „date confidențiale”. Prin urmare, ele intră nu doar sub incidența normelor generale pentru protecția datelor cu caracter personal din Legea privind protecția datelor cu caracter personal, ci și sub incidența normelor speciale de protecție privind prelucrarea categoriilor speciale de date cu caracter personal, conținute în articolele 3, 6 și 7 ale acestei legi.

Datele cu privire la sănătate sunt considerate toate datele medicale cu privire la factorii generali despre sănătatea persoanei. Aceste date, transformate în date statistice, pot fi folosite pentru monitorizarea și evaluarea sistemelor și politicilor cu privire la sănătate, pentru a stabili previziuni

<sup>3</sup> În cauza *Bodil Lindqvist*, Curtea de Justiție a Uniunii Europene a declarat că „precizarea faptului că o persoană s-a rănit la picior și lucrează cu fracțiune de normă pe motive medicale, constituie date cu caracter personal referitoare la starea de sănătate”.

bugetare, a face prospectivă în domeniul sănătății și a compara acești indicatori cu alții (mediu, produse alimentare, educație, utilizarea substanțelor psihotrope, alcoolismul, fumatul, etc.).

În absența unei definiții juridice „*datele cu caracter personal privind starea de sănătate*” ar putea fi definite ca orice informație referitoare la sănătatea fizică sau mentală a unei persoane, sau cu privire la furnizarea de servicii medicale pentru această persoană.

Protecția datelor cu caracter personal privind starea de sănătate este astăzi o temă majoră. Importanța acestui subiect provine de la exploatarea considerabilă a noilor tehnologii informaționale și comunicațiilor în sectorul medical. Utilizarea lor este susceptibilă de a fi benefică atât pacienților, cât și specialiștilor din domeniu, simplificând considerabil prelucrarea datelor cu caracter personal în domeniul medical. Evoluțiile tehnologice rapide permit de a stoca, prelucra și transmite către terți date cu caracter personal privind starea de sănătate la un nivel fără precedent. Dar revoluția digitală, de asemenea, poate crea noi riscuri ce pot aduce atingere drepturilor și libertăților cetățenilor.

## CAPITOLUL II

### MĂSURILE TEHNICO-ORGANIZATORICE AFERENTE OPERAȚIUNILOR DE PRELUCRARE A DATELOR CU CARACTER PERSONAL PRIVIND STAREA DE SĂNĂTATE A SUBIECȚILOR DE DATE

#### Puncte cheie:

- Cadrele medicale și personalul auxiliar din cadrul instituțiilor medicale urmează a fi supuși unei clauze de confidențialitate;
- Operatorii de date cu caracter personal urmează să elaboreze și să implementeze politica de securitate instituțională care stabilește normele de securitate a datelor cu caracter personal;
- Accesul la dosarele medicale ale subiecților de date va fi condiționat de informarea prealabilă, în scris, a persoanelor cărora se acordă accesul despre obligațiile ce le revin în conformitate cu prevederile art. 4, 29 și 30 ale Legii privind protecția datelor cu caracter personal.

1. Entităților implicate în domeniul sănătății, în dependență de rolul pe care îl au, se recomandă a le fi atribuită în actele normative departamentale, calitatea de operator, persoană împuternicită de operator sau destinatar, în conformitate cu noțiunile statuate de art. 3 al Legii privind protecția datelor cu caracter personal. Aceasta va permite delimitarea clară a competențelor și repartizarea adecvată a drepturilor și obligațiilor în cadrul operațiunilor de prelucrare a datelor cu caracter personal.

2. Toate cadrele medicale, care au acces la date cu caracter personal, urmează a fi supuse unei clauze de confidențialitate care, după caz, poate fi inclusă în contractele de muncă, având calitate de clauză contractuală, sau în fișele postului, cu mențiunea despre posibilitatea atragerii la răspundere civilă, contravențională ori penală pentru încălcarea acesteia.

3. Entitățile ce activează în domeniul sănătății (operatori de date cu caracter personal) sunt obligate să notifice CNPDCP, personal sau prin persoanele împuternicite, sistemele de evidență a datelor cu caracter personal, conform procedurii prevăzute la art. 23 al Legii privind protecția datelor cu caracter personal. Cadrele medicale, instituțiile medico-sanitare și personalul medical al acestora pot prelucra date cu caracter personal privind starea de sănătate fără autorizația CNPDCP numai dacă prelucrarea este necesară pentru protejarea vieții, integrității fizice sau a sănătății subiecților datelor cu caracter personal, conform prevederilor art. 7 alin. (2) din același act legislativ (spre exemplu, în cazul acordării primului ajutor medical).

4. Operatorii de date cu caracter personal urmează să elaboreze și să implementeze politica de securitate instituțională, în conformitate cu prevederile Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr. 1123 din 14 decembrie 2010 (Cerințe), care ar acoperi aspecte ce vizează: procedurile și măsurile legate de realizarea politicii de securitate, cu aplicarea soluțiilor practice cu un nivel de detalizare și complexitate proporțional; identificarea și autentificarea utilizatorilor investiți cu dreptul de acces la sistemele informaționale de date cu caracter personal prelucrate în procesul acordării asistenței medico-sanitare; modalitățile de reacționare la incidentele de securitate; de protecție a tehnologiei informaționale și comunicațiilor; de asigurare a integrității informației care conține date cu caracter personal și a tehnologiei informaționale; de administrare a accesului la datele cu caracter personal prelucrate; de audit în sistemele informaționale și de evidență a datelor cu caracter personal etc.

5. Politica de securitate urmează să conțină reglementări care ar asigura protecția datelor cu caracter personal, prelucrate în domeniul sănătății, în cadrul sistemelor de evidență, în special, prin următoarele metode:

1) preîntâmpinarea conexiunilor neautorizate la rețelele comunicaționale și interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste rețele, în special în procesul dezvoltării prin transmitere a datelor cu caracter personal între entitățile abilitate cu diferite



competențe în procesul de organizare a întregului sistem medical:

2) excluderea accesului neautorizat la datele cu caracter personal prelucrate în cadrul sistemelor de evidență prin metoda implementării procedurilor de identificare și autentificare a utilizatorilor; prin repartizarea obligațiilor și investirea cu minimul de drepturi și competențe a celor implicați în procesul de gestionare a sistemelor de evidență a datelor cu caracter personal; prin asigurarea integrității resurselor informaționale (*date și programe*);

3) preîntâmpinarea acțiunilor speciale tehnice și de program care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program, a soft-ului destinat prelucrării datelor cu caracter personal, prin metoda folosirii mijloacelor de protecție speciale tehnice și de program, inclusiv a programelor licențiate, programelor antivirus, organizării sistemului de control al securității soft-ului și efectuarea periodică a copiilor de siguranță;

4) preîntâmpinarea acțiunilor intenționate și/sau neintenționate a utilizatorilor interni și/sau externi, precum și a altor angajați, care condiționează distrugerea, modificarea datelor cu caracter personal prelucrate în cadrul sistemelor de evidență sau defecțiuni în lucrul complexului tehnic și de program;

5) preîntâmpinarea scurgerii de informații care conțin date cu caracter personal, transmise prin canalele de legătură, prin folosirea metodelor de cifrare (*criptare*) a acestei informații;

6) stabilirea exactă a ordinii și procedurilor de acces la informația care conține date cu caracter personal, prelucrată în cadrul sistemelor informaționale și de evidență, atât pentru utilizatorii interni, cât și pentru cei externi;

7) organizarea generării înregistrărilor de audit a securității în sistemele informaționale și de evidență a datelor cu caracter personal pentru a fi posibilă acumularea probatoriului în cazurile investigării eventualelor operațiuni de acces/tentativă de acces neautorizat, a operațiunilor de modificare, extragere, blocare, ștergere sau distrugere a datelor cu caracter personal prelucrate în sisteme de evidență.

6. În cazul dezvăluirii prin transmitere a formatului electronic al datelor cu caracter personal, conținute în dosarele pacienților, dosarele cadrelor instituțiilor medicale, documentele de asigurare obligatorie de asistență medicală prin rețele comunicaționale ori pe alt suport electronic (digital) de stocare, se va asigura criptarea acestei informații sau se va examina posibilitatea utilizării unei conexiuni bilaterale prin canal securizat VPN (rețele private virtuale). Accesul fără fir la sistemele informaționale de date cu caracter personal urmează a fi permis și autorizat doar în cazul utilizării mijloacelor criptografice de protecție a informației. Fiecare caz de solicitare a transmiterii datelor cu caracter personal pe cale electronică va fi examinat separat, reieșind din posibilitățile tehnice a destinatarului și operatorului, precum și în corespundere cu măsurile organizatorice și tehnice implementate de părți. În cazul în care rețelele comunicaționale prezintă riscuri pentru confidențialitatea și securitatea datelor cu caracter personal, vor fi utilizate metode tradiționale de transmitere (expediere poștală cu aviz recomandat, înmînarea personală, etc.)

7. Transmiterea datelor cu caracter personal care vizează pacienții/cadrelor instituțiilor medicale prin rețelele comunicaționale ce nu corespund Cerințelor, (spre exemplu: expedierea informației prin intermediul e-mail-urilor personale de tipul @gmail.com, @mail.ru, @yahoo.com, etc) urmează a fi interzisă. Se recomandă utilizarea rețelilor oficiale, spre exemplu: @ms.gov.md.

8. Procedura dezvăluirii prin transmitere a datelor cu caracter personal (*stocate atât pe suport de hîrtie, cât și electronic*), inclusiv în cazul colaborării internaționale în domeniul sănătății (*ex: în cadrul realizării proiectelor de acordare a asistenței medicale și de cercetare științifică, programelor de cooperare și asistență internațională, stagiilor de cercetare pentru profesori, masteranzi, doctoranzi*) urmează a fi reglementată prin act normativ instituțional, luîndu-se în considerare necesitatea asigurării unui nivel adecvat de protecție a datelor cu caracter personal, utilizînd inclusiv canalele diplomatice.

9. Transmiterea transfrontalieră a datelor cu caracter personal urmează a fi efectuată în strictă corespundere cu prevederile art. 32 al Legii privind protecția datelor cu caracter personal (ținînd cont de răspunderea contravențională, prevăzută de art. 74<sup>1</sup> Cod contravențional în aceste cazuri), în special în cazurile cînd tratatul internațional în baza căruia se efectuează transmiterea nu conține garanții privind protecția drepturilor subiectului de date cu caracter personal.

Volumul și categoria datelor cu caracter personal colectate în scopuri medicale și a altor acțiuni din domeniul sănătății, necesită a fi limitate la strictul necesar pentru realizarea scopurilor declarate.

**10.** Ministerul Sănătății, Muncii și Protecției Sociale urmează să reglementeze, la nivel național, procedura clară și specifică de acces la materialele dosarelor medicale ale pacienților, de acces în perimetrele de securitate în care sînt prelucrate date cu caracter personal și alte informații cu caracter medical, care conțin date cu caracter personal, în vederea neadmiterii dezvăluirii neautorizate a acestor date, inclusiv procedura și limitele în care pot fi efectuate filmări foto și video, ținîndu-se cont de necesitatea asigurării principiilor de confidențialitate și securitate a prelucrării datelor cu caracter personal, prevăzute de art. 29 și 30 ale Legii privind protecția datelor cu caracter personal, cu implementarea acestora de către fiecare operator ce activează în domeniul medical.

**11.** În caz de solicitare a accesului la dosarele medicale ale subiecților de date, persoanele cărora le este acordat accesul urmează a fi informate în scris despre obligațiile ce le revin în conformitate cu prevederile art. 4, 29 și 30 ale Legii privind protecția datelor cu caracter personal, inclusiv despre răspunderea prevăzută de art. 74<sup>1</sup> Cod contravențional.

**12.** Aceste măsuri trebuie să fie realizate prin intermediul unui contract sau angajament al părților, specificat în formă scrisă și formulat în conformitate cu prevederile Legii privind protecția datelor cu caracter personal, care, pe lângă informațiile, regulile și obligațiile ce vizează principiile de protecție a datelor cu caracter personal, ar stabili concret responsabilitatea ce urmează să și-o asume persoana care a primit acces la aceste date cu caracter personal în legătură cu prelucrarea ulterioară a acestora.

De asemenea, este necesar de asigurat echilibrul între dreptul la informare a publicului și obligația statului/operatorului de a asigura protecția datelor cu caracter personal, inclusiv în cazul prelucrării datelor prin diseminarea informațiilor publicului larg, ținîndu-se cont de faptul că în conformitate cu pct. 1 din anexa nr. 2 la Cerințe, operațiunile de prelucrare a datelor cu caracter personal privind starea de sănătate prezintă riscuri speciale pentru drepturile și libertățile acestora. **De exemplu:** în cazul știrilor diseminate în mass-media despre pacienții minori sau persoanele infectate cu HIV, filmările, fotografiile și interviurile efectuate în cadrul instituțiilor medicale cu implicarea în unele cazuri a personalului, fără a solicita, în prealabil, consimțământul de la persoanele vizate sau reprezentanții lor legali, constituie o încălcare a intimității și vieții private, precum și a principiilor de protecție a datelor cu caracter personal.

Este important ca în timpul efectuării unor investigații jurnalistice să fie garantat dreptul la inviolabilitatea vieții intime, familiale și private (*art.28 din Constituția Republicii Moldova*), precum și regimul de confidențialitate și de securitate a prelucrării datelor cu caracter personal (*art.29 și 30 din Legea privind protecția datelor cu caracter personal*), regim care se anulează doar în cazul depersonalizării acestor date. Din aceste considerente, folosirea tehnicii foto, video, audio sau altor mijloace de înregistrare a datelor cu caracter personal ale pacienților, în cadrul și pe teritoriul instituțiilor medicale, poate fi admisă doar în baza consimțământului subiectului de date cu caracter personal vizat (*în cazul prelucrării datelor acestuia prin intermediul mijloacelor video/foto/audio*) sau în cazul prezenței unei permisiuni speciale din partea conducerii ierarhice a operatorului de date cu caracter personal (*atunci când aceste operațiuni ar putea viza datele cu caracter personal prelucrate de angajați în formă automatizată sau neautomatizată, cum ar fi înregistrarea video/foto a cartelor medicale aflate pe masa de lucru, a ecranelor calculatorului, etc.*), care trebuie să-și asume responsabilitatea pentru eventualele prejudicii morale și materiale, aduse subiecților de date cu caracter personal.

**13.** Prelucrarea categoriilor speciale de date cu caracter personal ale pacienților (*spre exemplu: vizita la medicul specialist, tratamentul acordat, rezultatele investigații medicale, complicații, etc.*) este interzisă, în afara excepțiilor prevăzute de art. 6 din Legea privind protecția datelor cu caracter personal.

Accesul la astfel de date urmează a fi strict reglementat și trebuie să se limiteze la pacienți, iar în cazul incapacității de exercițiu sau al capacității de exercițiu limitate a acestora, la reprezentanții lor legali, la instituțiile medicale, personalul medico-sanitar, asistenții sociali și organele de poliție, în cazurile prevăzute expres de lege.

14. Datele privind starea de sănătate a pacienților fac parte din categoria specială de date cu caracter personal. Din acest motiv, trebuie să se respecte cu strictețe principiile prevăzute de art. 7 din Legea privind protecția datelor cu caracter personal. Aceste date urmează să fie prelucrate doar de personalul medical, care are obligația de a le cunoaște, fiind supuși secretului profesional ori de către sau sub supravegherea unei alte persoane supuse unei obligații echivalente în ceea ce privește secretul profesional, inclusiv principiilor etice în baza procedurilor statuate în Codurile de conduită profesională.

15. Operatorii de date cu caracter personal trebuie să respecte principiile generale pentru protecția datelor cu caracter personal, reglementate de cadrul legislativ în materie de protecție a datelor cu caracter personal, și anume:

1) Datele trebuie prelucrate într-o manieră transparentă, legală și echitabilă.

2) Datele trebuie colectate în scopuri explicite, specifice și legitime și nu trebuie prelucrate într-o manieră incompatibilă cu aceste scopuri. Prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri științifice sau istorice de cercetare sau în scopuri statistice nu este considerată incompatibilă cu scopurile inițiale, atunci când garanțiile adecvate permit respectarea drepturilor și libertăților fundamentale.

3) Prelucrarea datelor trebuie să fie proporțională cu scopul legitim urmărit și trebuie să se realizeze numai în baza unui temei legal sau a consimțământului subiectului de date cu caracter personal.

4) Datele cu caracter personal privind starea de sănătate, trebuie în principiu și în măsura posibilităților, să fie colectate de la subiectul de date. În cazul în care subiectul de date nu este în măsură să furnizeze datele și aceste date sunt necesare în scopul prelucrării, ele pot fi colectate din alte surse legale, în conformitate cu principiul legalității prelucrării datelor cu caracter personal.

5) Datele trebuie să fie adecvate, relevante și neexcesive în raport cu scopurile pentru care sunt prelucrate; acestea trebuie să fie exacte și, dacă este necesar, să fie actualizate.

6) În temeiul art. 30 din Legea privind protecția datelor cu caracter personal, operatorului de date îi revine obligația de a stabili măsuri de securitate adecvate. Operatorii de date trebuie să aplice măsuri tehnice și organizatorice corespunzătoare pentru a proteja datele cu caracter personal împotriva distrugerii, modificării, blocării, copierii, răspîndirii, precum și împotriva altor acțiuni ilicite, măsuri menite să asigure un nivel de securitate adecvat în ceea ce privește riscurile prezentate de prelucrare și caracterul datelor prelucrate. Aceste măsuri de tip organizațional și tehnic urmează a fi implementate ținându-se cont de ultimele evoluții tehnologice, de natura sensibilă a datelor privind starea de sănătate și evaluarea potențialelor riscuri.

7) Respectarea drepturilor subiecților de date cu caracter personal, reglementate de Legea privind protecția datelor cu caracter personal.

### **CAPITOLUL III**

#### **CADRUL LEGAL CARE GUVERNEAZĂ OPERAȚIUNILE DE PRELUCRARE A DATELOR CU CARACTER PERSONAL PRIVIND STAREA DE SĂNĂTATE A SUBIECȚILOR DE DATE**

##### **Puncte cheie:**

- Datele cu caracter personal privind starea de sănătate nu pot fi colectate și prelucrate decât în conformitate și cu asigurarea garanțiilor adecvate prevăzute de legislația în vigoare.
- Principiile de protecție a datelor cu caracter personal privind starea de sănătate trebuie respectate de către toți operatorii, indiferent că își desfășoară activitatea în domeniul public sau cel privat, inclusiv de către persoanele împuternicite, astfel încât să fie realizat obiectivul final de respectare a drepturilor subiecților de date.
- Informația despre starea sănătății care are caracter personal, precum și datele despre starea pacientului, rezultatele investigațiilor, diagnosticul, pronosticul, tratamentul, sînt date confidențiale și urmează a fi protejate de către medicii, personalul medico-sanitar.



farmacistii și de către toate persoanele care intră în posesia unor date cu caracter personal privind starea de sănătate a subiectului.

## **1. Temeiurile legale ale prelucrării datelor referitoare la sănătate**

1) Temeiurile de prelucrare a datelor cu caracter personal privind starea de sănătate intră sub incidența dispozițiilor speciale reglementate prin art. 6 și 7 ale Legii privind protecția datelor cu caracter personal. Astfel, prelucrarea datelor cu caracter personal privind starea de sănătate va dispune de legalitate în măsura în care operatorul de date își va fundamenta operațiunea de prelucrare pe cel puțin unul dintre următoarele temeiuri legale:

a) subiectul datelor cu caracter personal și-a dat consimțământul. În cazul subiectului datelor cu caracter personal în privința căruia a fost instituită măsura de ocrotire judiciară sub forma tutelei, prelucrarea categoriilor speciale de date cu caracter personal se efectuează numai cu obținerea consimțământului în formă scrisă al tutorelui;

b) prelucrarea este necesară pentru îndeplinirea obligațiilor sau drepturilor specifice ale operatorului în domeniul dreptului muncii, cu respectarea garanțiilor prevăzute de lege și ținându-se cont de faptul că o eventuală dezvăluire către un terț a datelor cu caracter personal prelucrate în acest scop poate fi efectuată numai dacă există o obligație legală a operatorului în acest sens;

c) prelucrarea este necesară pentru protecția vieții, integrității fizice sau a sănătății subiectului datelor cu caracter personal ori a altei persoane, în cazul în care subiectul datelor cu caracter personal se află în incapacitate fizică sau juridică de a-și da consimțământul;

d) prelucrarea este efectuată în contextul activităților legitime de către asociații obștești, partide și alte organizații social-politice, de către sindicate, asociații de patronat, organizații filozofice sau religioase, organizații cooperatiste necomerciale, cu condiția ca prelucrarea să se refere numai la membrii acestora sau la persoanele cu care acestea au contacte permanente în legătură cu scopurile lor și cu condiția ca datele să nu fie dezvăluite terților fără consimțământul subiecților datelor cu caracter personal;

e) prelucrarea se referă la date făcute publice în mod voluntar și manifest de către subiectul datelor cu caracter personal;

f) prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în justiție al subiectului datelor cu caracter personal;

g) prelucrarea este necesară în scopul asigurării securității statului, cu condiția ca aceasta să se efectueze cu respectarea drepturilor subiectului datelor cu caracter personal și a celorlalte garanții prevăzute de prezenta lege;

h) prelucrarea este necesară în scopuri de medicină preventivă, de stabilire a diagnosticelor medicale, de administrare a unor îngrijiri sau tratamente pentru subiectul datelor cu caracter personal sau de gestionare a serviciilor de sănătate care acționează în interesul subiectului datelor cu caracter personal;

i) prelucrarea este necesară pentru protecția sănătății publice.

2) De asemenea, datele cu caracter personal privind starea de sănătate vor fi prelucrate prin prisma art. 4 și 5 ale Legii privind protecția datelor cu caracter personal. *Spre exemplu, datele referitoare la sănătate pot fi prelucrate, inclusiv, în cazul în care prelucrarea este necesară pentru executarea unui contract încheiat între subiectul de date sau în numele său cu un profesionist din domeniul sănătății, în condițiilor definite de lege, inclusiv sub obligația de păstrare a secretului.*

În toate cazurile, trebuie stabilite garanții adecvate pentru a asigura, în special, securitatea datelor și respectarea drepturilor persoanelor.

## **2. Colectarea și prelucrarea datelor cu caracter personal**

1) Respectarea drepturilor și libertăților fundamentale, inclusiv a dreptului la viața privată, trebuie să fie garantat atunci când se efectuează colectarea și prelucrarea datelor cu caracter personal privind starea de sănătate.

2) În principiu, colectarea și prelucrarea datelor privind starea de sănătate trebuie să fie efectuate numai de către cadre medicale sau de către persoane sau entități care acționează în numele acestor specialiști.

3) Operatorii care nu sînt specialiști în domeniul sănătății trebuie să colecteze și să prelucereze date cu caracter personal privind starea de sănătate doar cu respectarea fie a regulilor de confidențialitate echivalente cu cele ce revin unui cadru medical, fie a garanțiilor eficiente prevăzute de legislația în vigoare.

4) Colectarea și prelucrarea datelor cu caracter personal privind starea de sănătate trebuie să fie efectuată într-un mod corect și conform prevederilor legii, și numai în scopuri determinate, explicite și legitime.

5) Dacă datele cu caracter personal privind starea de sănătate au fost colectate în scopuri de medicină preventivă sau de stabilire a diagnosticelor medicale, de administrare a unor îngrijiri sau tratamente pentru subiectul datelor cu caracter personal, ele pot fi, de asemenea, prelucrate în scopuri de gestionare a serviciilor medicale, în cazul în care gestionarea este efectuată de un cadru medical care a colectat datele, sau dacă datele sunt comunicate unei persoane supuse secretului profesional.

#### **Notă**

*Informația compilată în fișele de evidență a bolnavilor, în registre de evidență etc., precum: numele, prenumele persoanei fizice, IDNP ș.a. fac posibilă identificarea directă a unei persoane fizice și, respectiv, sînt considerate date cu caracter personal, fiind protejate de Legea privind protecția datelor cu caracter personal.*

6) Principiile de prelucrare a datelor cu caracter personal trebuie respectate de către toți operatorii, indiferent că își desfășoară activitatea în domeniul public sau cel privat, inclusiv de către persoanele împuternicite, astfel încât să fie realizat obiectivul final de respectare a drepturilor persoanelor vizate.

7) În virtutea celor menționate, CNPDCP recomandă reglementarea concretă a aspectelor legate de protecția datelor cu caracter personal și a mecanismelor de implementare a acestora în activitatea curentă a instituțiilor medicale în conformitate cu prevederile Legii privind protecția datelor cu caracter personal și a Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărîrea Guvernului nr. 1123 din 14 decembrie 2010.

### **3. Informarea subiecților de date cu caracter personal**

1) În cazul în care datele cu caracter personal sunt colectate direct de la subiectul datelor, operatorul sau persoana împuternicită de către operator este obligată să-i furnizeze următoarele informații, exceptând cazul în care acesta deține deja informațiile respective:

- a) identitatea operatorului sau, după caz, a persoanei împuternicite de către operator;
- b) scopul prelucrării datelor colectate;
- c) informații suplimentare, precum:

- destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
- existența drepturilor de acces la date, de intervenție asupra datelor și de opoziție, precum și condițiile în care acestea pot fi exercitate;
- dacă răspunsurile la întrebările cu ajutorul cărora se colectează datele sînt obligatorii sau voluntare, precum și consecințele posibile ale refuzului de a răspunde.

2) În cazul în care datele cu caracter personal nu sunt colectate direct de la subiectul datelor, operatorul sau persoana împuternicită de către operator este obligată ca, în momentul colectării datelor sau, dacă se intenționează dezvăluirea acestora către terți, cel mai târziu în momentul primei dezvăluiri, să furnizeze subiectului datelor cu caracter personal informația privind categoriile de date care urmează a fi colectate sau dezvăluite, precum și informațiile indicate supra.

### **Notă**

*În cazul în care datele cu caracter personal privind starea de sănătate nu sînt colectate direct de la persoana vizată, aceasta urmează să fie informată despre colectarea lor cît mai rapid posibil, în mod corespunzător, cu excepția cazului cînd furnizarea informațiilor este imposibilă sau implică un efort disproporționat față de interesul legitim care ar putea fi lezat.*

3) În cazul în care persoana vizată este o persoană cu incapacitate de exercițiu sau cu capacitate de exercițiu limitată și nu este în măsură să decidă de sine stătător, și dacă legea nu-i permite să acționeze în nume propriu, informațiile trebuie transmise reprezentantului legal în interesul persoanei vizate.

4) Derogări de la prevederile expuse supra pot fi făcute în următoarele cazuri:

a) informarea persoanei vizate poate fi limitată, dacă derogările sunt prevăzute prin lege și dacă ele constituie o măsură necesară într-o societate democratică:

- la prevenirea unui pericol iminent sau pentru înlăturarea unei infracțiuni;
- pentru protecția sănătății publice;
- pentru protejarea persoanei vizate și a drepturilor și libertăților altora.

b) în caz de urgență medicală, datele considerate ca necesare pentru aplicarea tratamentului medical pot fi colectate înainte de a informa persoana.

5) Ulterior consumării circumstanțelor care au generat aplicarea derogărilor expuse supra, operatorul de date cu caracter personal urmează să informeze subiectul de date cu caracter personal vizavi de prelucrarea datelor sale cu caracter personal.

## **4. Consimțământul**

1) Potrivit art. 3 din Legea privind protecția datelor cu caracter personal, consimțământul subiectului datelor cu caracter personal reprezintă orice manifestare de voință liberă, expresă și necondiționată, în formă scrisă sau electronică, conform cerințelor documentului electronic, prin care subiectul datelor cu caracter personal acceptă să fie prelucrate datele care îl privesc.

Din definiția legală a consimțământului, sunt desprinse următoarele elemente constitutive ale acestuia: a) liber exprimat; b) specific; c) informat; d) lipsit de ambiguitate prin care subiectul de date cu caracter personal acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care îl privesc să fie prelucrate.

**a) liber exprimat** - elementul liber exprimat implică o alegere reală și un control real din partea subiectului de date. Dacă subiectul de date cu caracter personal nu beneficiază de o opțiune reală, se simte obligat sau constrâns să-și exprime consimțământul pentru prelucrarea datelor cu caracter personal, sau intimidat de diverse consecințe negative care pot surveni în cazul în care nu-și exprimă consimțământul, acesta nu va fi valabil.

Dacă consimțământul este integrat, ca parte ce nu poate fi negociată, în cuprinsul termenelor și condițiilor contractuale, se prezumă că acesta nu a fost exprimat în mod liber. În consecință, consimțământul nu va fi considerat liber exprimat dacă subiectul de date nu este în măsură să refuze sau să-și retragă consimțământul fără a fi prejudiciat. Atunci când se evaluează dacă consimțământul este exprimat în mod liber, trebuie să se țină seama, de asemenea, de situația specială în care consimțământul este inclus în contracte sau dacă prestarea unui serviciu este condiționată de acordarea consimțământului. În termeni generali, orice element de presiune sau de influență nepotrivită asupra persoanei vizate (care se poate manifesta în diferite moduri) și care împiedică exprimarea voinței libere a acesteia determină lipsa de validitate a consimțământului.

b) **specific** - trebuie să privească o situație bine delimitată, concretă, unde este avută în vedere prelucrarea datelor medicale. În consecință „un acord general” al subiectului de date privind colectarea datelor sale medicale și al transferului ulterior al acestor date medicale către cadre medicale implicate în tratament nu constituie un consimțământ în sensul noțiunii redată în art. 3 din Legea

privind protecția datelor cu caracter personal.

Pentru a respecta condiția referitoare la elementul „specific”, operatorul trebuie să aplice:

- specificarea scopului ca măsură de protecție împotriva utilizării datelor cu caracter personal în alte scopuri incompatibile cu cel stabilit inițial;
- granularitatea în solicitările de consimțământ;
- separarea clară a informațiilor referitoare la obținerea consimțământului pentru activitățile de prelucrare a datelor de informațiile referitoare la alte chestiuni.

Obținerea unui consimțământ valabil este precedată întotdeauna de stabilirea unui scop specific, explicit și legitim pentru activitatea de prelucrare preconizată. Consimțământul trebuie să fie specific scopului. Subiecții de date își vor da consimțământul, înțelegând că dețin controlul și că datele lor vor fi prelucrate numai în scopurile care au fost menționate. Dacă un operator prelucrează date privind starea de sănătate pe baza consimțământului și dorește să prelucereze datele într-un alt scop, operatorul respectiv trebuie să solicite un nou consimțământ pentru acest alt scop, cu excepția cazului în care există un alt temei legal care să reflecte mai bine situația.

c) **informat** – element constitutiv care este conexas cu cerința transparenței operațiunilor de prelucrare a datelor cu caracter personal. Furnizarea de informații persoanelor vizate înainte de obținerea consimțământului acestora este esențială pentru a le permite să ia decizii în cunoștință de cauză, să înțeleagă aspectele față de care își exprimă acordul și, de exemplu, să își exercite dreptul de a-și retrage consimțământul. Dacă operatorul nu furnizează informații accesibile, controlul subiectului de date devine iluzoriu, iar consimțământul nu va constitui un temei valabil pentru prelucrare. Consecința nerespectării cerințelor referitoare la consimțământul în cunoștință de cauză constă în faptul că respectivul consimțământ nu va fi valabil.

d) **lipsit de ambiguitate** - consimțământul necesită o declarație din partea subiectului de date sau o acțiune echivocă, ceea ce înseamnă că acesta trebuie întotdeauna să fie dat printr-o manifestare activă de voință sau printr-o declarație. Trebuie să fie evident că persoana vizată a acordat consimțământul pentru o anumită prelucrare. În același sens, consimțământul urmează să fie precis, clar și să nu existe prezența simultană a mai multor sensuri care să genereze multiple interpretări.

2) De asemenea, un operator trebuie să fie conștient de faptul că consimțământul nu poate fi obținut prin aceeași acțiune prin care se consimte la încheierea unui contract sau se acceptă termenele și condițiile generale ale unui serviciu. Acceptarea în alb a termenelor și condițiilor generale nu poate fi considerată drept o acțiune fără echivoc de a consimți prelucrarea datelor cu caracter personal. Operatorii trebuie să elaboreze mecanisme de consimțământ clare pentru persoanele vizate, să evite ambiguitatea și să se asigure că acțiunea prin care este acordat consimțământul se poate deosebi de alte acțiuni.

## 5. Dreptul de acces, rectificare și opoziție a subiecților de date

1) Persoanei, în calitate de subiect de date cu caracter personal, trebuie să-i fie asigurat accesul la datele sale cu caracter personal privind starea de sănătate, fie direct, fie prin intermediul unei persoane desemnate în acest sens, dacă legislația în vigoare permite. Informațiile trebuie să fie accesibile și într-o formă inteligibilă.

În această ordine de idei, art. 11 alin. (4) din Legea cu privire la drepturile și responsabilitățile pacientului stipulează că, prestatorii de servicii de sănătate asigură accesul nelimitat al pacientului, al reprezentatului său legal la informația privind propriile date medicale, la rezultatele și la dosarele cu investigații, la tratamentele și îngrijirile primite, cu eliberarea unui rezumat în scris la externare. Pacientul poate obține copia oricărei părți din propriile date și dosare medicale în modul stabilit de Ministerul Sănătății, Muncii și Protecției Sociale. Procedura este stabilită prin ordinul Ministerului Sănătății nr. 303 din 06 mai 2010 „Cu privire la asigurarea accesului la informația privind propriile date medicale și lista intervențiilor medicale care necesită perfectarea acordului informat”.

2) Urmează a remarcă, că potrivit prevederilor pct. 13 lit. a) din ordinul nominalizat, cererea scrisă, depusă de solicitant, trebuie să conțină datele de identificare a solicitantului, iar pct. 14 lit. a) din același ordin stipulează că, cererea este însoțită de copia buletinului de identitate a solicitantului.



### **Notă**

*În acest context, de menționat că, în activitatea sa, CNPDCP adesea este sesizat de subiecții de date cu caracter personal cu privire la solicitarea din partea reprezentanților instituțiilor medicale de a anexa la cerere copia buletinului de identitate.*

*Practica condiționării obținerii copiei buletinului de identitate de la subiecții datelor cu caracter personal și atașarea acestuia, spre exemplu, la o cerere în scop de a demonstra identitatea solicitantului – este o situație de fapt eronată și nefondată pe alocuri din punct de vedere al scopului pentru care se obține această copie, fiind colectate excesiv date cu caracter personal care nu se atribuie la caz, în această situație fiind necesară blurarea/excluderea datelor cu caracter personal excesive scopului reglementat, ținând cont de prevederile art. 4 alin. (1) al Legii nr. 133 din 08 iulie 2011 privind protecția datelor cu caracter personal, care prevede că datele cu caracter personal care fac obiectul prelucrării trebuie să fie :*

*a) prelucrate în mod corect și conform prevederilor legii;*

*b) colectate în scopuri determinate, explicite și legitime, iar ulterior să nu fie prelucrate într-un mod incompatibil cu aceste scopuri;*

*c) adecvate, pertinente și neexcesive în ceea ce privește scopul pentru care sunt colectate și/sau prelucrate ulterior; etc.*

*Atragem atenția că, identificatorii consemnați în copiile buletinului de identitate reprezintă un risc sporit din motiv că aceștia produc efecte juridice pe un termen nelimitat (în anumite situații chiar și după decesul titularului de drept), precum și faptul că de pe aceste copii sunt făcute alte copii care ar putea fi utilizate cu totul în alte scopuri (ilegale) decât cele pentru care au fost colectate.*

*Pornind de la circumstanțele menționate, CNPDCP nu a identificat temeiul legal care ar împuternici reprezentanții instituției medicale cu dreptul de a solicita copia buletinului de identitate și de a prelucra un volum impunător de date cu caracter personal conținute în buletinele de identitate în cadrul examinării cererii de eliberare a informației privind propriile date medicale. Or, în acest context, instituția medicală urmează să utilizeze buletinul de identitate doar pentru a identifica pacientul/persoana care solicită informațiile de ordin medical și, eventual, a transcrie datele necesare asigurării unei evidențe privind eliberarea informațiilor, fără a colecta copiile de pe aceste acte.*

3) Accesul persoanei vizate la datele cu caracter personal privind starea de sănătate poate fi refuzat, limitat sau amânat doar în cazurile prevăzute de lege.

4) Subiectul datelor cu caracter personal poate cere de la operator rectificarea datelor eronate care îl vizează sau/și actualizarea lor și, în caz de refuz, trebuie să aibă posibilitatea de a contesta acțiunile sau inacțiunile acestuia/acestora în organul abilitat cu apărarea drepturilor subiecților datelor cu caracter personal – Centrul Național pentru Protecția Datelor cu Caracter Personal sau în instanța de judecată.

## **6. Dezvăluirea datelor către terți**

1) Potrivit prevederilor art. 12 din Legea nr. 263-XVI din 27 octombrie 2005 cu privire la drepturile și responsabilitățile pacientului, toate datele privind identitatea și starea pacientului, rezultatele investigațiilor, diagnosticul, pronosticul, tratamentul, precum și datele cu caracter personal sînt confidențiale și urmează a fi protejate și după moartea acestuia.

Potrivit alin. (3) al art. 12 al Legii nr. 263-XVI din 27 octombrie 2005 cu privire la drepturile și responsabilitățile pacientului informațiile ce se consideră confidențiale pot fi furnizate numai în cazul în care pacientul consimte acest lucru în mod explicit sau la solicitarea reprezentantului său legal (a rudei apropiate), în condițiile consimțite de pacient, în măsură adecvată capacității lui de înțelegere, în situații cînd capacitatea de exercițiu a pacientului nu este deplină sau lipsește ori dacă legea o cere în

mod expres.

2) Conform art. 14 al Legii ocrotirii sănătății, medicii, personalul medico-sanitar, farmaciștii sînt obligați să păstreze secretul informațiilor referitoare la boală, la viața intimă și familială a pacientului de care au luat cunoștință în exercițiul profesiei, cu excepția cazurilor de pericol al răspîndirii maladiilor transmisibile, la cererea motivată a organelor de urmărire penală sau a instanțelor judecătorești.

3) Corespunzător prevederilor art. 8 CEDO, orice persoană are dreptul la respectarea vieții sale private și de familie, a domiciliului său și a corespondenței sale. Nu este admis amestecul unei autorități publice în exercitarea acestui drept, decît în măsura în care acest amestec este prevăzut de lege și dacă constituie o măsură, care într-o societate democratică este necesară pentru securitatea națională, siguranța publică, bunăstarea economică a țării, apărarea ordinii și prevenirea faptelor penale, protejarea sănătății sau a morale, ori protejarea drepturilor și libertăților altora.

Subsecvent, menționăm că în conformitate cu prevederile art. 6 alin. (1) din Legea privind protecția datelor cu caracter personal, prelucrarea categoriilor speciale de date cu caracter personal (din care fac parte și datele cu caracter personal privind starea de sănătate) este interzisă, cu excepția anumitor condiții descrise la acest articol.

Articolul 7 din același act legislativ stipulează că, datele cu caracter personal privind starea de sănătate pot fi preluate în scopuri de medicină preventivă, de stabilire a diagnosticilor medicale, de administrare a unor îngrijiri sau tratamente pentru subiectul datelor cu caracter personal sau de gestionare a serviciilor de sănătate în interesul subiectului datelor cu caracter personal, de către sau sub supravegherea unui cadru medical supus secretului profesional ori de către sau sub supravegherea unei alte persoane supuse unei obligații echivalente în ceea ce privește secretul profesional.

#### **Nota**

*Datele cu caracter personal privind starea de sănătate, precum rezultatele investigațiilor, diagnosticul, pronosticul, tratamentul, sînt date confidențiale și urmează a fi protejate, iar medicii, personalul medico-sanitar, farmaciștii, sînt obligați să păstreze secretul informațiilor referitor la boala, la viața intimă și familială a pacientului de care au luat cunoștință în exercițiul profesiei, cu excepția cazurilor de pericol al răspîndirii maladiilor transmisibile, la cererea motivată a organelor de urmărire penală sau a instanțelor judecătorești.*

4) Accesul la datele cu caracter personal privind starea de sănătate trebuie să fie efectuat în baza temeiurilor legale cu demonstrarea unei legături de cauzalitate între datele la care este solicitat accesul și necesitatea acestora pentru scopul declarat.

5) Trebuie adoptate măsuri speciale pentru a preveni ca pacienții să fie determinați să-și dezvăluie datele cu caracter personal privind starea de sănătate, *de exemplu, la solicitarea unui viitor angajator sau a unei societăți private de asigurări. Instruirea pacientului este esențială pentru a preveni răspunsul favorabil la asemenea solicitări, care pot fi ilegale potrivit Legii privind protecția datelor cu caracter personal.*

6) Datele cu caracter personal privind starea de sănătate nu trebuie comunicate către terți, cu excepția condițiilor enumerate mai jos sau în cazul anonimizării lor.

7) În cazul în care legislația în vigoare prevede alte garanții corespunzătoare, dezvăluirea datelor cu caracter personal cu privire la starea de sănătate poate avea loc numai dacă beneficiarul este supus regulilor de confidențialitate specifice cadrului medical sau obligațiilor echivalente în ceea ce privește secretul medical, și cu respectarea dispozițiilor prezentei instrucțiuni.

8) Datele cu caracter personale privind starea de sănătate pot fi dezvăluite dacă ele sunt pertinente și:

a) dacă dezvăluirea este statuată prin lege și constituie o măsură necesară într-o societate democratică în scopurile:

- protecției sănătății publice; sau

- prevenirii unui pericol iminent sau pentru înlăturarea unei infracțiuni; sau
- unui alt interes public important; sau
- protecției drepturilor și libertăților altor persoane;
- b) dacă legea autorizează dezvăluirea în scopurile:
  - protecției persoanei vizate sau a unei rude pe linie genetică; sau
  - salvarea unui interes vital al persoanei vizate sau a unei persoane terțe; sau
  - respectarea unei obligații contractuale determinate; sau
  - constatării, exercitării sau apărării unui drept în instanță.

c) dacă persoana vizată sau reprezentantul său legal, sau o autoritate, sau orice altă persoană sau instanță desemnată prin lege și-a dat acordul pentru unul sau mai multe scopuri și cu condiția ca legislația în vigoare să nu interzică;

d) cel puțin ca persoana vizată sau reprezentantul său legal sau o autoritate, sau orice altă persoană sau instanță desemnată prin lege să nu se opună expres, în cazul în care datele au fost colectate în scopuri de medicină preventivă, diagnosticare sau terapie și dacă scopul dezvăluirii nu este incompatibil cu scopul prelucrării pentru care au fost colectate datele, inclusiv în scopul efectuării îngrijirii pacientului sau de gestionare al unui serviciu sanitar acționând în interesul pacientului.

11) În situații generale, fiecare caz de dezvăluire a datelor cu caracter personal, indiferent de statutul solicitantului (olășter de urmărire penală, procuror, deputat, judecător, etc.) trebuie analizat de operator pentru identificarea:

a) scopului concret pentru care se solicită dezvăluirea acestor date și dacă acest scop este în legătură cu cel pentru care au fost colectate sau nu;

b) volumului, categoriilor și structurii concrete a datelor cu caracter personal la care se solicită accesul, astfel încât să fie asigurată proporționalitatea și necesitate între scopul declarat și datele la care este solicitat acces;

c) cadrului normativ care întemeiază cererea de acces a solicitantului la aceste informații;

d) argumentelor privind necesitatea acestor informații oficiale cu accesibilitate limitată;

e) prezenței temeiurilor prevăzute de art. 5, 6 sau 7 ale Legii privind protecția datelor cu caracter personal, care motivează punerea la dispoziție terților a informației cu caracter confidențial, în absența consimțământului subiectului datelor cu caracter personal;

f) posibilității aplicării prevederilor art. 31 al actului legislativ pre citat, privind depersonalizarea datelor cu caracter personal puse la dispoziția terților (după analiza detaliată a scopurilor pentru care se solicită accesul la aceste date).

Totodată, luând în considerație faptul că prelucrarea datelor cu caracter personal privind starea de sănătate prezintă riscuri speciale pentru persoana fizică în partea ce vizează inviolabilitatea vieții intime, familiale și private ale acesteia, este absolut necesară asigurarea unui nivel de confidențialitate și securitate sporit al acestora, de către persoanele care au acces la ele.

12) Entitățile care solicită accesul la datele cu caracter personal prelucrate în sistemele de evidență gestionate de instituțiile medico-sanitare, urmează să indice în demersurile sale nu doar prevederile legale care întemeiază aceste operațiuni, dar și să demonstreze executarea preventivă a obligațiilor legale în vederea asigurării regimului de confidențialitate și securitate a prelucrării datelor cu caracter personal, în conformitate cu prevederile art. 29-30 ale Legii privind protecția datelor cu caracter personal.

13) Instituțiile medicale au obligația legală, prescrisă de dispozițiile Legii nr. 263-XVI din 27 octombrie 2005 cu privire la drepturile și responsabilitățile pacienților, Legii ocrotirii sănătății nr. 411-XIII din 28 martie 1995, Legii nr. 1402-XIII din 16 decembrie 1997 privind sănătatea mentală, Legii nr. 264-XVI din 27 octombrie 2005 cu privire la exercitarea profesiei de medic, precum și prevederile Codului de procedură penală (art. 15, art. 214), de a analiza minuțios legalitatea acordării accesului, transmiterii sau dezvăluirii datelor, cu întreprinderea acțiunilor și măsurilor necesare în vederea asigurării confidențialității și securității prelucrării acestora, întrucât poartă întreaga răspundere pentru nerespectarea acestui regim, inclusiv și pentru neindicarea prescripțiilor necesare a fi urmate de destinatarii datelor cu caracter personal.

### **Notă**

*Nu se pune la îndoială dreptul și importanța datelor cu caracter personal privind starea de sănătate, pentru anumiți operatori, în situații legale de exercitare a activității sale, spre exemplu pentru organele de drept. Însă, adesea, reieșind din conținutul interpelărilor ofițerilor de urmărire penală, acestea conțin informații insuficiente și nu oferă pentru operatorii de date cu caracter personal (instituțiile medicale) garanții că, datele cu caracter personal privind starea de sănătate a persoanei fizice, dezvăluite, vor fi corect administrate și sînt necesare pentru o anumită cauză contravențională penală.*

*Astfel, nu este suficient de a regăsi în conținutul demersurilor doar cadrul temeiului juridic relevant care întemeiază cererea de acces la informații oficiale cu accesibilitate limitată, dar acestea trebuie să cuprindă și scopul concret pentru care se solicită dezvăluirea categoriilor speciale de date cu caracter personal, care ar oferi o justificare suficientă pentru ingerința în viața privată a persoanei fizice, legătura cauzală și/sau calitatea procesuală a persoanelor, datele cu caracter personal ale cărora se solicită, față de dosarul cauza contravențională penală.*

## **7. Securitatea datelor personale și obligația operatorilor de înregistrare în calitate de operator de date cu caracter personal în Registrul de evidență al operatorilor de date cu caracter personal**

### **7.1. Securitatea**

7.1.1. Măsurile de protecție a datelor cu caracter personal reprezintă o parte componentă a lucrărilor de creare, dezvoltare și exploatare a sistemului informațional de date cu caracter personal și vor fi efectuate neîntrerupt de către toți deținătorii de date cu caracter personal.

7.1.2. Protecția datelor cu caracter personal în sistemele informaționale de date cu caracter personal, indiferent de forma ținerii acestora (*în continuare sisteme informaționale*), trebuie asigurată printr-un complex de măsuri tehnice și organizatorice de preîntâmpinare a prelucrării ilicite a datelor cu caracter personal.

7.1.3. Măsurile de protecție a datelor cu caracter personal prelucrate în sistemele informaționale de date cu caracter personal se înfăptuiesc ținându-se cont de necesitatea asigurării confidențialității acestor măsuri.

7.1.4. Înfăptuirea oricăror măsuri și lucrări cu folosirea resurselor informaționale ale operatorului de date cu caracter personal este interzisă în cazurile în care nu sunt adoptate și implementate măsuri corespunzătoare de protecție a datelor cu caracter personal.

7.1.5. Sunt supuse protecției toate resursele informaționale ale operatorilor de date cu caracter personal, care conțin date cu caracter personal, inclusiv:

a) suporturile magnetice, optice, laser sau alte suporturi ale informației electronice, masive informaționale și baze de date;

b) sistemele informaționale, rețelele, sistemele operaționale, sistemele de gestionare a bazelor de date și alte aplicații, sistemele de telecomunicații, inclusiv mijloacele de confecționare și multiplicare a documentelor și alte mijloace tehnice de prelucrare a informației.

7.1.6. Protecția datelor cu caracter personal în sistemele informaționale de date cu caracter personal este asigurată în scopul:

a) preîntâmpinării scurgerii informației care conține date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta;

b) preîntâmpinării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în rețelele telecomunicaționale și resursele informaționale;

c) respectării cadrului normativ de folosire a sistemelor informaționale și a programelor de prelucrare a datelor cu caracter personal;

d) asigurării caracterului complet, integru, veridic al datelor cu caracter personal în rețelele telecomunicaționale și resurselor informaționale;



c) păstrării posibilităților de gestionare a procesului de prelucrare și păstrare a datelor cu caracter personal.

7.1.7. Protecția datelor cu caracter personal prelucrate în sistemele informaționale se efectuează prin următoarele metode:

a) preîntâmpinarea conexiunilor neautorizate la rețelele telecomunicaționale și interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste rețele;

b) excluderea accesului neautorizat la datele cu caracter personal prelucrate;

c) preîntâmpinarea acțiunilor speciale tehnice și de program, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program;

d) preîntâmpinarea acțiunilor intenționate și/sau neintenționate a utilizatorilor interni și/sau externi, precum și a altor angajați ai operatorului de date cu caracter personal, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program.

7.1.8. Preîntâmpinarea scurgerii de informații care conțin date cu caracter personal, transmise prin canalele de legătură, este asigurată prin folosirea metodelor de cifrare a acestei informații, inclusiv cu utilizarea măsurilor organizaționale, tehnice și de regim.

7.1.9. Preîntâmpinarea accesului neautorizat la informațiile care conțin date cu caracter personal și circulă sau se păstrează în mijloace tehnice este asigurată prin metoda folosirii mijloacelor speciale tehnice și de program, cifrării acestor informații, inclusiv prin măsurile organizaționale și de regim.

7.1.10. Preîntâmpinarea distrugerii, modificării datelor cu caracter personal sau defecțiunilor în funcționarea soft-ului destinat prelucrării datelor cu caracter personal este asigurată prin metoda folosirii mijloacelor de protecție speciale tehnice și de program, inclusiv a programelor licențiate, programelor antivirus, organizării sistemului de control al securității soft-ului și efectuarea periodică a copiilor de siguranță.

7.1.11. Ordinea de acces la informația care conține date cu caracter personal, identificarea și autentificarea utilizatorilor sistemelor informaționale de date cu caracter personal, administrarea accesului utilizatorilor, auditul securității în sistemele informaționale de date cu caracter personal, copiile de rezervă și restabilirea informației care conține date cu caracter personal, gestionarea incidentelor de securitate a sistemelor informaționale de date cu caracter personal, etc. se efectuează de către operatorul de date cu caracter personal, în conformitate cu Cerințele față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr. 1123 din 14 decembrie 2010 și alte acte normative. În cazul formei manuale de ținere a registrelor în care sunt prelucrate seriile structurate de date cu caracter personal, accesibile conform criteriilor centralizate sau descentralizate, ori repartizate conform criteriilor funcționale sau geografice, operatorii de date cu caracter personal vor aplica prevederile Cerințelor menționate, cu excepția pct.11-13, 23, 25, 27, 30-32, 35, 37-44, 46, 49, 51-53, 55-68, 72-77, 80, 87-89 și 91.

## **7. 2. Interoperabilitatea**

7.2.1. Interoperabilitatea oferă posibilitatea diferitelor sisteme informatice de a comunica și de a schimba date și poate contribui la soluționarea nevoilor importante din sectorul medical. De asemenea, poate contribui la consolidarea protecției datelor privind starea de sănătate și, în cele din urmă, a persoanelor fizice, în special prin furnizarea de mijloace tehnice pentru a facilita actualizarea informațiilor sau pentru a evita stocarea datelor identice în mai multe baze de date și pentru a contribui la portabilitatea datelor.

7.2.2. Cu toate acestea, este necesar ca interoperabilitatea să fie realizată în deplină conformitate cu principiile prevăzute de legislația în vigoare, în special principiile legalității, necesității și proporționalității și să se introducă măsuri de protecție a datelor atunci când se utilizează sisteme interoperabile.

### **7. 3. Obligația operatorilor de înregistrare în calitate de operator în Registrul de evidență al operatorilor de date cu caracter personal și de notificare a sistemelor de evidență gestionate**

7.3.1. Operatorii care prelucrează date cu caracter personal privind starea de sănătate trebuie, să elaboreze politica instituțională de securitate a datelor cu caracter personal și regulamente interne în vederea respectării recomandărilor enunțate în prezentele instrucțiuni în conformitate cu prevederile Legii privind protecția datelor cu caracter personal și a Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr. 1123 din 14 decembrie 2010.

7.3.2. Prevederile art. 23 și art. 28 ale Legii privind protecția datelor cu caracter personal, impun obligația ca anterior inițierii operațiunilor de prelucrare a datelor cu caracter personal într-un sistem de evidență automatizat sau manual, acestea să fie notificate CNPDCP. Notificarea trebuie să conțină următoarele informații:

a) numele sau denumirea și domiciliul ori sediul în Republica Moldova ale operatorului și ale persoanei împuternicite de către acesta, dacă este cazul;

b) scopul prelucrării;

c) descrierea subiecților datelor cu caracter personal, descrierea datelor ce vor fi prelucrate, precum și a surselor de proveniență a acestor date;

d) existența consimțământului subiectului datelor cu caracter personal privind prelucrarea acestora;

e) modul în care subiecții datelor cu caracter personal sînt informați asupra drepturilor lor: data estimată pentru încheierea operațiunilor de prelucrare, precum și destinația ulterioară a datelor cu caracter personal;

f) destinatarii cărora se intenționează să li se dezvăluie datele cu caracter personal;

g) garanțiile privind transmiterea datelor cu caracter personal către terți;

h) propuneri privind transferurile transfrontaliere ale datelor cu caracter personal care se intenționează să fie făcute;

i) persoanele responsabile pentru prelucrarea datelor cu caracter personal;

j) specificarea sistemelor de evidență a datelor cu caracter personal care au legătură cu prelucrarea, precum și a eventualelor legături cu alte prelucrări de date sau cu alte sisteme de evidență a datelor cu caracter personal, indiferent dacă se efectuează sau nu, respectiv dacă sînt situate sau nu pe teritoriul Republicii Moldova;

k) motivele care justifică aplicarea prevederilor art.10 și art.12 alin. (3), în situația în care prelucrarea datelor se face exclusiv în scopuri jurnalistice, artistice sau literare ori în scopuri statistice, de cercetare istorică sau științifică;

l) descrierea generală a măsurilor luate pentru asigurarea securității prelucrării datelor cu caracter personal conform prevederilor art. 30.

În cazul în care datele cu caracter personal care sînt prelucrate urmează să fie transferate către alte state, notificarea va cuprinde suplimentar:

a) categoriile de date care vor face obiectul transferului;

b) statul de destinație pentru fiecare categorie de date.

7.3.3. Punctul 21 din Regulamentul Registrului de evidență a operatorilor de date cu caracter personal, aprobat prin Hotărârea Guvernului nr. 296 din 15 mai 2012 stabilește că fiecare sistem de evidență a datelor cu caracter personal se notifică separat. În acest sens, operatorului de date cu caracter personal îi revine obligația de a identifica și a înregistra toate sistemele de evidență gestionate.

7.3.4. În scopul facilitării procedurii de înregistrare în calitate de operator de date cu caracter personal și notificare a sistemelor de evidență a datelor cu caracter personal, CNPDCP a elaborat Ghidul privind procedura înregistrării operatorilor și a sistemelor de evidență a datelor cu caracter personal<sup>4</sup>. De asemenea, procedura de completare a notificării este descrisă în Manualul operatorului și în Ghidul video privind notificarea în Registrul de evidență a operatorilor de date cu caracter personal, elaborate de CNPDCP, care pot fi vizualizate accesând link-ul: <http://datepersonale.md/md/pan/>

<sup>4</sup> [http://datepersonale.md/md/proc\\_nof/](http://datepersonale.md/md/proc_nof/)

7.3.5. Potrivit art. 30 al Legii privind protecția datelor cu caracter personal, în cazul în care prelucrarea datelor cu caracter personal este efectuată pe seama și în numele operatorului, acesta va împuternici o persoană care va asigura respectarea garanțiilor referitoare la măsurile adecvate de securitate tehnică și de organizare privind prelucrarea ce urmează să fie efectuată.

7.3.6. Prelucrarea datelor cu caracter personal prin intermediul persoanei împuternicite de către operator trebuie reglementată printr-un contract sau un alt act juridic care să asigure în special faptul că:

- a) persoana împuternicită acționează numai pe baza instrucțiunilor operatorului;
- b) obligațiile privind asigurarea măsurilor organizatorice și tehnice necesare pentru protecția datelor cu caracter personal împotriva distrugerii, modificării, blocării, copierii, răspândirii, precum și împotriva altor acțiuni ilicite îi revin și persoanei împuternicite.

## **8. Stocarea**

În linii generale, datele cu caracter personal privind starea de sănătate nu trebuie stocate decât pe perioada necesară pentru atingerea scopurilor pentru care au fost colectate și prelucrate.

1) Condițiile și termenele de stocare a datelor cu caracter personal se stabilesc de legislație ținându-se cont de prevederile art. 4 alin. (1) lit. e) din Legea privind protecția datelor cu caracter personal. La expirarea termenului de stocare, datele cu caracter personal urmează a fi distruse în modul stabilit de lege.

2) Datele cu caracter personal din registrele de stat, de la data încetării utilizării acestora, pot rămâne la păstrare primind statutul de document de arhivă.

3) La încheierea operațiunilor de prelucrare a datelor cu caracter personal, dacă subiectul acestor date nu și-a dat consimțământul pentru o altă destinație sau pentru o prelucrare ulterioară, acestea vor fi:

- a) distruse;
- b) transferate unui alt operator, cu condiția ca operatorul inițial să garanteze faptul că prelucrările ulterioare au scopuri similare celor în care s-a făcut prelucrarea inițială;
- c) transformate în date anonime și stocate exclusiv în scopuri statistice, de cercetare istorică sau științifică.

4) După decesul subiectului datelor cu caracter personal, datele acestuia se pot utiliza:

- cu consimțământul, acordat în formă scrisă, de către succesorii acestuia;
- în scop de arhivă; sau
- în alte scopuri prevăzute de lege.

5) În cazul în care datele cu caracter personal privind starea de sănătate care nu mai sînt utilizate în scopul declarat inițial, dar sînt necesare în interesul protecției sănătății publice, cercetării științifice, istorice, statistice sau în scopuri pentru a permite operatorului sau persoanei împuternicite de operator să exercite sau să apere drepturile sale în justiție, se va face cu respectarea garanțiilor privind prelucrarea datelor cu caracter personal, prevăzute de normele ce reglementează aceste domenii, și numai pentru perioada necesară realizării acestor scopuri.

6) La cererea persoanei vizate, datele cu caracter personal privind starea de sănătate, urmează a fi șterse, cu excepția cazului cînd acestea sînt transformate în date anonime sau sînt utilizate în interese superioare și legitime, în corespundere cu prevederile legii, sau datele cu caracter personal sînt supuse arhivării.

## **9. Transmiterea transfrontalieră**

1) Prin prisma prevederilor art. 4 și art. 5 ale Legii privind protecția datelor cu caracter personal, drept condiție de bază la transmiterea transfrontalieră a datelor cu caracter personal este existența consimțământului subiectului de date, manifestat liber, expres și necondiționat, în formă scrisă sau electronică, conform cerințelor documentului electronic, prin care subiectul datelor consimte să fie transmise transfrontalier datele cu caracter personal care îl vizează.

Astfel, potrivit Deciziei nr. 176 din 15 iulie 2015, în cazul existenței consimțământului subiectului de date, autorizarea de către CNPDCP a transmiterii transfrontaliere a datelor cu caracter personal, inclusiv a celor privind starea de sănătate nu este necesară.

2) Totodată, transmiterea transfrontalieră a datelor cu caracter personal privind starea de sănătate care fac obiectul unei prelucrări sau care urmează să fie prelucrate după transmitere, poate avea loc cu autorizarea CNPDCP, în modul stabilit de lege, și doar în cazul în care statul de destinație asigură un nivel adecvat de protecție a drepturilor subiecților datelor cu caracter personal și a datelor destinate transmiterii.

3) Transmiterea transfrontalieră a datelor cu caracter personal privind starea de sănătate fără autorizarea CNPDCP poate avea loc în cazul în care transferul datelor cu caracter personal se face în baza prevederilor unei legi speciale sau ale unui tratat internațional ratificat de Republica Moldova. Legea specială sau tratatul internațional trebuie să conțină garanții privind protecția drepturilor subiectului datelor cu caracter personal.

3) CNPDCP recomandă regăsirea în textul tratatului internațional a prevederilor referitoare la:

a) caracteristica datelor, prevăzute de art. 5 din Convenția nr. 108 și art. 4 din Legea privind protecția datelor cu caracter personal;

b) drepturile subiectului de date cu caracter personal, cum ar fi: dreptul la informare, dreptul de acces la date, dreptul de intervenție asupra datelor cu caracter personal, dreptul de opoziție al persoanei vizate, prevăzute de art. 12- 18 din Legea privind protecția datelor cu caracter personal;

c) obligațiunile părților de a asigura securitatea și confidențialitatea datelor cu caracter personal care constituie obiect al transmiterii transfrontaliere;

d) posibilitatea de a se adresa instanței de judecată și/sau autorității de supraveghere a prelucrării datelor cu caracter personal.

3) Respectiv, în situația în care legea specială ori tratatul internațional nu conține garanții privind protecția drepturilor subiecților datelor cu caracter personal, transmiterea transfrontalieră a datelor cu caracter personal, prin prisma art. 32 alin. (7) al Legii privind protecția datelor cu caracter personal nu poate avea loc, decât cu autorizarea CNPDCP.

4) Prin derogare de la art. 32 din Legea privind protecția datelor cu caracter personal, transferul transfrontalier de date privind starea de sănătate către un stat care nu asigură un nivel adecvat de protecție a datelor în conformitate cu Convenția nr. 108 și cu prezentele instrucțiuni nu trebuie efectuat, cel puțin dacă:

a) nu fost luate măsuri necesare, inclusiv contractuale, privind respectarea prevederilor Convenției nr. 108 și că subiectul datelor cu caracter personal nu a avut posibilitatea de a se opune transferului; sau

b) subiectul datelor cu caracter personal nu și-a dat consimțământul său.

5) În cazul unui transfer de urgență sau acceptat de către subiectul datelor cu caracter personal, atunci când datele privind starea de sănătate sînt transferate de la o țară la alta, trebuie luate măsuri adecvate pentru a asigura protecția acestora, în special:

a) responsabilul pentru transfer trebuie să indice destinatarului scopurile pentru care datele au fost colectate inițial și persoanele sau organizațiile cărora le pot fi comunicate;

b) cu excepția cazului în care legislația prevede altfel, beneficiarul trebuie să se angajeze față de responsabil să respecte scopurile stabilite și legitime și să nu comunice datele altor persoane sau entități, decât cele specificate de responsabilul de transfer.

## **9. Cercetarea științifică**

1) Un alt domeniu cu implicații considerabile cu privire la protecția datelor cu caracter personal este acel al studiilor clinice și a celor de cercetare medicală.

În măsura posibilităților, datele cu caracter personal privind starea de sănătate prelucrate în scopuri de cercetare științifică trebuie să fie anonime. Instituțiile de specialitate și științifice implicate, precum și autoritățile publice trebuie să promoveze dezvoltarea tehnicilor și procedurile care asigură anonimatul. Depersonalizarea poate fi un mijloc adecvat pentru a răspunde nevoilor științifice și, în



același timp, protejează interesele pacienților în cauză. Astfel, în conformitate cu prevederile art. 31 din Legea privind protecția datelor cu caracter personal, în scopuri statistice, de cercetare istorică, științifică, sociologică, medicală, de documentare juridică, operatorul depersonalizează datele cu caracter personal prin retragerea din ele a părții care permite identificarea persoanei, transformându-le în date anonime, care nu pot fi asociate cu o persoană identificată sau identificabilă. În cazul depersonalizării, regimul de confidențialitate stabilit pentru datele respective se anulează.

#### **Notă**

*Spitalele și medicii pot transmite date din fișele medicale ale pacienților lor la o societate în scopul efectuării unor cercetări medicale, cu condiția existenței unui temei legal de prelucrare a datelor cu caracter personal.*

*Nici un nume al pacienților nu este utilizat, iar fiecărui caz clinic i se atribuie la întâmplare număr de serie, pentru a asigura coerență și pentru a evita confuzia între informațiile referitoare la diferiți pacienți. Numele pacienților rămân, în mod exclusiv, în posesia medicilor respectivi care sunt obligați să păstreze secretul profesional. Datele nu cuprind nici o informație suplimentară care să facă posibilă identificarea pacienților prin combinarea acestora. În plus, s-au luat toate măsurile necesare pentru a preveni identificarea persoanelor vizate sau posibilitatea ca acestea să devină identificabile, fie că este vorba despre măsuri juridice, tehnice sau organizaționale. În aceste circumstanțe, se poate aprecia că nu există mijloace care pot fi utilizate, în mod rezonabil, pentru a identifica persoanele vizate."*

2) În cazul în care anonimatul ar face imposibilă realizarea unui proiect de cercetare științifică, iar proiectul trebuie să se desfășoare în scopuri legitime, cercetarea ar putea fi realizată cu utilizarea datelor cu caracter personal, cu condiția ca:

a) subiectul datelor cu caracter personal să-și dea consimțământul pentru scopurile cercetării; sau

b) în cazul în care subiectul datelor cu caracter personal se află în incapacitate juridică și nu este capabil de decizii libere, iar legislația în vigoare nu - i permite să acționeze în nume propriu, atunci reprezentantul său legal sau o autoritate, sau orice persoană sau instanță desemnată prin lege, își dă consimțământul în cadrul proiectului de cercetare în legătură cu starea de sănătate sau boala persoanei vizate; sau

c) comunicarea datelor în scopuri de cercetare științifică, necesare pentru protecția sănătății publice este autorizată de unul sau mai multe autorități desemnate de lege, dar numai:

- dacă subiectul datelor cu caracter personal nu s-a opus expres comunicării; și

- dacă nu este posibilă, în pofida eforturilor rezonabile, de a lua contact cu subiectul datelor cu caracter personal pentru a colecta consimțământul lui; și

- dacă interesele proiectului de cercetare justifică această autorizare; sau

d) ca cercetarea științifică să fie prevăzută de lege și să constituie o măsură necesară pentru protecția sănătății publice.

3) Sub rezerva condițiilor prevăzute de legislația în vigoare, cadrele medicale autorizate să efectueze propriile lor cercetări medicale trebuie să poată utiliza datele cu caracter personal privind starea de sănătatea pe care le dețin cu condiția ca subiectul datelor cu caracter personal să fi fost informat cu privire la această posibilitate și nu are careva obiecții.

4) Datele cu caracter personal utilizate în scopuri de cercetare științifică, pot fi publicate într-o formă care să permită identificarea subiecților datelor cu caracter personal, cu condiția existenței consimțământului subiecților de date cu caracter personal.