00323/07/EN
WP 131

Document de lucru privind prelucrarea datelor medicale cu caracter personal din dosarul electronic de sănătate (DES)

Adoptat la 15 februarie 2007

Grupul de lucru a fost înființat conform articolului 29 din Directiva 95/46/CE. Este un organism consultativ european independent privind protecția datelor şi confidențialitatea. Activitățile sale sunt descrise în articolul 30 din Directiva 95/46/CE şi articolul 15 din Directiva 2002/58/CE.

Secretariatul este asigurat de către Directoratul C (Justiție Civilă, drepturi şi cetățenie) al Comisiei Europene, Directoratul General pentru Justiție, libertate şi securitate, B-1049 Bruxelles, Belgia, Biroul No LX-46 01/43.

Adresă de Internet: http://europa.eu.int/comm/justice_home/fsj/privacy/index_en.htm

R E Z U M A T

În acest Document de lucru privind **prelucrarea datelor medicale cu caracter personal din dosarul electronic de sănătate (DES),** Grupul de lucru pentru articolul 29 oferă asistență în interpretarea cadrului legal în vigoare privind protecția datelor pentru sistemele DES şi explică unele dintre principiile sale generale. Documentul de lucru oferă şi indicații privind cerințele de protecție a datelor pentru înființarea sistemelor DES, precum şi a măsurilor de protecție aplicabile.

La început, Grupul de lucru pentru articolul 29 examinează **cadrul general privind protecția datelor pentru sistemele DES**. Grupul de lucru pentru articolul 29 reaminteşte existența interdicției generale pentru prelucrarea datelor medicale cu caracter personal din articolul 8 alineatul (1) din Directiva 95/46/CE privind protejarea datelor, şi apoi discută posibila aplicare a derogărilor prevăzute la articolul 8 alineatele (2), (3) şi (4) ale directivei în contextul sistemelor DES, accentuând necesitatea interpretării unor asemenea derogări într-o manieră strictă.

Grupul de lucru pentru articolul 29 reflectează şi asupra **cadrului legal adecvat pentru sistemele DES** şi oferă **recomandări în privința a unsprezece situații** în care măsurile speciale de protecție din sistemele DES se pot dovedi necesare pentru a garanta drepturile de protecție ale datelor pacienților şi indivizilor. Aceste situații sunt:

1. Respectarea autodeterminării
2. Identificarea şi autentificarea pacienților şi a personalului medical
3. Autorizarea accesării DES pentru citirea şi introducerea de date în DES
4. Utilizarea DES în alte scopuri
5. Structura de organizare a unui sistem DES
6. Categorii de date stocate în DES şi modul de prezentare a acestora
7. Transferul internațional al dosarelor medicale
8. Securitatea datelor
9. Transparența
10. Răspunderea
11. Mecanismele de control pentru prelucrarea datelor în DES

Grupul de lucru pentru articolul 29 invită medicii, tot personalul medical, toate persoanele şi instituțiile implicate în procesul medical, precum şi publicul larg, să îşi prezinte observațiile asupra acestui Document de lucru.

CUPRINS

GRUPUL DE LUCRU PENTRU PROTECȚIA PERSOANELOR FIZICE PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL,

Având în vedere Directiva 95/46/CE a Parlamentului European şi a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi libera circulație a acestor date [1], în special articolele 29 şi 30, alineatul 1 litera (b),

Având în vedere Regulamentul de Procedură al Grupului de lucru[2], în special articolele 12 şi 14,

A ADOPTAT URMĂTORUL DOCUMENT DE LUCRU:

I. Introducere

Obiectivul acestui Document de lucru al Grupului de lucru pentru articolul 29 este de a oferi asistență în interpretarea cadrului legal în vigoare privind protecția datelor pentru sistemele DES şi de a stabili anumite principii generale. Avizul mai doreşte să evidențieze condițiile prealabile pentru înființarea unui sistem DES național, precum şi a măsurilor de protecție aplicabile.

Costurile sistemelor publice de asistență medicală se află în creştere dramatică iar guvernele solicită noi strategii pentru rezolvarea acestei probleme. Una dintre soluțiile care se evidențiază tot mai frecvent este "dosarul electronic de sănătate (DES)". Termenii utilizați în acest domeniu includ "dosarul electronic medical (DEM)", "dosarul electronic al pacientului (DEP)", "dosarul electronic de sănătate (DES)", "dosarul computerizat al pacientului (DCP)" etc. Aceşti termeni pot fi utilizați alternativ.

În sensul acestui Document de lucru, un "dosar electronic de sănătate (denumit în continuare: DES)" se defineşte ca

> *"Un dosar medical complet sau o documentație similară a stării de sănătate din trecut şi prezent, fizice şi psihice a unei persoane fizice, în format electronic, care oferă accesul prompt la aceste date în scop de tratament medical sau în alte scopuri similare*[3]*."*

În mod tradițional, documentația privind tratamentele medicale era disponibilă la unele cadre medicale, dar nu se reunea într-un dosar unic. Spre deosebire, conceptul de "DES" intenționează să compileze documentația existentă privind tratamentele medicale ale unei persoane din surse şi perioade diferite. Astfel, vor fi furnizate date cât mai detaliate posibil despre starea de sănătate din trecut şi prezent a unei persoane, pentru o perioadă de timp considerabilă, probabil pentru toată viața ("*de la naştere până la moarte").* După compilare,

---

[1] Directiva 95/46/CE a Parlamentului European şi a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi libera circulație a acestor date; JO L 281, 23.11.1995, p. 31 (în continuare: „directiva"); disponibilă la: http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm.

[2] Adoptat de către Grupul de lucru la a treia sa întrunire, la 11.9.1996.

[3] „Tratamentul medical şi obiectivele similare" se referă la obiectivele menționate în articolul 8 alineatul (3) din directivă.

datele DES vor fi puse la dispoziția tuturor cadrelor medicale şi instituțiilor autorizate, în format electronic, oriunde şi oricând aceste date sunt necesare.

DES este considerat a fi mijlocul cel mai potrivit pentru

- a oferi un tratament de calitate mai bună în urma primirii unor date corecte despre pacient;
- ameliorarea eficienței din punct de vedere al costurilor tratamentelor medicale, prevenind astfel creşterea accentuată a deficitelor bugetare pentru sănătate;
- furnizarea datelor necesare pentru controlul calității, statistică şi planificare în sectorul de sănătate publică, cu rezultate benefice pentru bugetele de sănătate publică.

Răspunsurile la un chestionar din anul 2005, care a circulat între autoritățile de supraveghere a protejării datelor, a demonstrat că sistemele naționale DES sunt probleme importante şi urgente în majoritatea statelor membre. Gradul de punere în aplicare al unor asemenea sisteme diferă totuşi semnificativ: în timp ce în majoritatea statelor membre există o dezbatere privind DES, altele au pus în aplicare deja sistemele DES, cel puțin parțial.

Datorită faptului că serviciile medicale sunt furnizate tot mai mult şi peste frontieră, Comisia Europeană a subliniat în comunicatul său "*e-Health – asistență medicală mai eficientă pentru cetățenii Europei: Un plan de acțiune pentru zona europeană e-Health* "[4], importanța serviciilor e-Health şi a interoperabilității dosarelor electronice de sănătate. În afară de aceasta, Comunitatea Europeană finanțează proiecte în această privință, cum ar fi dosare electronice ale pacienților sau identificatori ai pacienților (de ex. Cardul european pentru asigurări de sănătate). În procesul de punere în aplicare a unor asemenea programe, Comisia Europeană are obligația, împreună cu statele membre, să asigure compatibilitatea cu toate prevederile legale relevante privind protecția datelor cu caracter personal şi, unde este cazul, să introducă mecanismele necesare pentru asigurarea confidențialității şi protejării unor asemenea date[5].

Sistemele DES au potențialul de a oferi o calitate şi securitate mai mare a datelor medicale decât formele tradiționale de documentație medicală. Cu toate acestea, din punctul de vedere al protejării datelor, trebuie accentuat faptul că sistemele DES mai au potențialul nu doar de a prelucra mai multe date cu caracter personal (de ex. în noi contexte, sau prin agregare), dar şi de a oferi mai prompt datele despre pacient unui cerc mai larg de destinatari decât era posibil până în acel moment.

Mai trebuie remarcat că datele medicale electronice dintr-un sistem DES – cu excepția accesibilității pentru cadrele medicale – pot fi de interes, în general, pentru terțe părți precum societăți de asigurări şi organisme de apărare a legii. Din punctul de vedere al protejării datelor cu caracter personal, în cursul compilării datelor medicale existente ale unei persoane din surse diferite, în scopul asigurării unui acces mai facil şi mai larg la aceste date confidențiale, sistemele DES prezintă un nou risc, oferind noi posibilități pentru eventuala utilizare incorectă a datelor medicale personale. Deşi acest nou risc va fi cunoscut pe deplin în majoritatea proiectelor doar în cursul unei aplicări complete viitoare, este totuşi necesar să fim conştienți de acest pericol acum, când majoritatea modelelor existente au doar o aplicare limitată sau parțială (de ex. doar pentru un set de bază de date medicale sau doar pentru spitale dintr-o anumită regiune), deoarece ele vor deveni general aplicabile într-o anumită perioadă de timp.

[4] COM (2004) 356 final.

[5] A se vedea, de ex. articolul 5 alineatul (5) din Decizia 1786/2002/CE.

II. Cadrul de protejare a datelor pentru dosarele electronice de sănătate

Orice prelucrare a datelor cu caracter personal în sistemele DES trebuie să respecte regulile de protejare a datelor cu caracter personal. Grupul de lucru doreşte să accentueze faptul că acest cadru aplicabil pentru utilizarea DES este prezentat în expunerea de motive nr. 2 din directivă, care afirmă că *"sistemele de prelucrare a datelor sunt în serviciul omului; (...) acestea trebuie, indiferent de naţionalitatea sau locul de reşedinţă al persoanelor fizice, să le respecte drepturile şi libertăţile fundamentale, în special dreptul la viaţă privată, şi să contribuie la progresul economic şi social, la dezvoltarea comerţului şi la bunăstarea persoanelor"*.

Dreptul fundamental la protejarea datelor cu caracter personal se întemeiază, în esenţă, pe articolul 8 din Convenţia europeană pentru apărarea drepturilor omului şi a libertăţilor fundamentale (CEDOLF) şi pe articolul 8 din Carta Europeană a Drepturilor Fundamentale[6]. Reguli mai specifice sunt expuse în Directiva 95/46/CE privind protejarea datelor şi în Directiva 2002/58/CE privind confidenţialitatea comunicaţiilor electronice[7], şi în legile interne ale statelor membre care aplică aceste directive.

Orice prelucrare a datelor cu caracter personal în DES trebuie să respecte şi regulile prevăzute de Convenţia pentru protejarea indivizilor cu privire la prelucrarea automată a datelor cu caracter personal a Consiliului Europei (ETS nr. 108) şi protocolul adiţional la Convenţia 108 privind autorităţile de control şi fluxurile de date transfrontaliere (ETS nr. 181).

În contextul DES, Grupul de lucru doreşte să atragă atenţia asupra Recomandării Consiliului Europei nr. R(97) 5 privind protecţia datelor medicale (13 februarie 1997). Se face referire şi la recomandările din „Grupul de lucru pentru accesul online al dosarelor electronice de sănătate" de către Grupul de lucru internaţional pentru protecţia datelor în telecomunicaţii[8].

1. Principii generale

Managerii de date care colectează date pentru aplicaţiile DES trebuie să respecte toate principiile generale pentru protecţia datelor, inclusiv următoarele:

- Să utilizeze principiul limitării (principiul scopului): Acest principiu inclus parţial în articolul 6 alineatul (1) litera (b) din directivă, printre altele, interzice continuarea prelucrării incompatibile cu scopul(urile) colectării.
- Principiul calităţii datelor: Acest principiu din directivă impune ca datele personale să fie relevante şi să nu depăşească scopurile în care sunt colectate. Astfel, orice date nerelevante nu trebuie să fie colectate, iar dacă au fost colectate, trebuie să fie distruse (articolul 6 alineatul (1) litera (c)). Mai este impusă obligaţia ca aceste date să fie exacte şi actualizate.

---

[6] Dreptul de protecţie al datelor cu caracter personal nu este absolut, şi poate fi restrâns dacă anumite interese publice o reclamă. Cu toate acestea, obiectivele de interes public pot justifica încălcarea protecţiei datelor cu caracter personal doar dacă aceasta se face conform legii, fiind necesară într-o societate democratică în scopul respectării intereselor de securitate naţională, a siguranţei publice sau bunăstării economice a ţării, pentru prevenirea dezordinii şi infracţiunilor, pentru protejarea sănătăţii publice şi moravurilor, sau pentru protejarea drepturilor şi libertăţilor altora, şi dacă nu depăşeşte obiectivul urmărit (articolul 8 alineatul (2) CEDOLF).

[7] Directiva 2002/58/CE a Parlamentului European şi Consiliului din 12 iulie 2002 privind prelucrarea datelor cu caracter personal şi protejarea vieţii private în sectorul comunicaţiilor publice (Directiva privind protecţia vieţii private şi comunicaţiile electronice) (JO L 201, 31.7.2002, p. 37–47).

[8] Adoptată la cea de a 39-a întrunire din Washington D.C., 6-7 aprilie 2006 (http://www.berlin-privacy-group.org).

- Principiul retenției: acest principiu cere ca datele cu caracter personal să nu fie stocate pentru o perioadă mai lungă decât este necesar pentru scopul în care aceste date au fost colectate şi prelucrate.
- Condiții de informare: În conformitate cu articolul 10 din directivă, managerii de date care prelucrează date în sistemele DES trebuie să furnizeze anumite date subiecților datelor, precum dezvăluirea identității managerului, a scopurilor prelucrării, a destinatarilor datelor şi a existenței unui drept de acces.
- Dreptul de acces al subiecților informației: articolul 12 din directivă permite subiecților informației să verifice corectitudinea datelor şi să se asigure că acestea sunt actualizate. Aceste drepturi se aplică în întregime în cazul colectării de date personale în sistemele DES.
- Obligații privind securitatea: articolul 17 din directivă obligă managerii de date să aplice măsuri tehnice şi organizatorice corespunzătoare pentru a proteja datele cu caracter personal împotriva distrugerii accidentale sau intenționate sau a transmiterii neautorizate. Aceste măsuri pot fi de tip organizațional sau tehnic.

2. Protecția specială pentru datele confidențiale cu caracter personal

Cu toate acestea, când prelucrarea unor astfel de date cu caracter personal privesc sănătatea unei persoane, prelucrarea este delicată şi reclamă, prin urmare, protecție specială.

> Definiția datelor cu caracter personal din articolul 2 (a) din Directiva 95/46/CE este următoarea:
>
> *"date cu caracter personal înseamnă orice informație referitoare la o persoană fizică identificată sau identificabilă ("persoană vizată"); o persoană identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un număr de identificare sau la unul sau mai multe elemente specifice identității sale fizice, fiziologice, psihice, economice, culturale sau sociale".*
>
> Definiția categoriilor speciale de date din articolul 8 alineatul (1) din directivă este următoarea:
>
> *"Statele membre interzic prelucrarea datelor cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, convingerile religioase sau filosofice, apartenența sindicală, precum şi prelucrarea datelor privind sănătatea sau viața sexuală."*

Menționarea faptului că o persoană s-a rănit la picior şi se află în repaos din considerente medicale constituie date cu caracter personal privind starea de sănătate în sensul articolului 8 alineatul (1) din directivă[9]. Această definiție se aplică şi datelor cu caracter personal când acestea au o legătură clară şi apropiată cu descrierea stării de sănătate a unei persoane: datele privind consumul de medicamente, alcool sau droguri, precum şi datele genetice sunt, fără îndoială, "date cu caracter personal privind starea de sănătate", în special dacă sunt incluse într-un dosar medical. De asemenea, orice alte date – de ex. datele administrative (numărul de asigurări sociale, data internării în spital etc) – aflate în documentația medicală a pacientului vor fi considerate ca fiind confidențiale: dacă nu ar fi fost relevante în contextul medical al pacientului, ele nu ar fi trebuit incluse în dosarul medical.

---

[9] Curtea de Justiție a Comunităților Europene, Hotărârea din 6 noiembrie 2003, cauza C-101/01 - Bodil Lindqvist.

În consecință, membrii Grupului de lucru consideră că toate datele conținute în documentația medicală, în dosarul electronic de sănătate şi în sistemele DES trebuie considerate a fi „date confidențiale cu caracter personal”. Prin urmare, ele se află nu doar sub incidența regulilor pentru protecția datelor cu caracter personal din directivă, ci şi sub incidența regulilor speciale de protecție privind prelucrarea datelor confidențiale conținute în articolul 8 din directivă.

3. O interdicție generală a prelucrării datelor medicale cu caracter personal – cu derogări

Articolul 8 alineatul (1) din Directiva 95/46/CE privind protejarea datelor interzice prelucrarea datelor cu caracter personal privind starea de sănătate în general. Este cazul şi articolului 6 din Convenția nr. 108 a Consiliului Europei.

Protecția specială conținută în articolul 8 alineatul (1) completează celelalte prevederi ale acestei directive, în special ale articolului 6, privind principiile referitoare la calitatea datelor, şi ale articolului 7, privind criteriile de legitimare a prelucrării datelor.

Cu toate acestea, având în vedere importanța utilizării informației despre un pacient în scopul tratării lui medicale eficiente, există excepții de la interdicția generală de prelucrare a datelor medicale.

Directiva privind protecția datelor prevede **derogările mandatorii** prevăzute în articolul 8 alineatele (2) şi (3) plus o **excepție opțională** din articolul 8 alineatul (4).

Toate aceste derogări sunt **limitate**, **exhaustive** şi se **interpretează în manieră strictă**.

4. Articolul 8 alineatul (2) litera (a): “Consimțământul explicit”

Conform articolului 8 alineatul (2) litera (a) din directivă:

> *“Alineatul 1 nu se aplică în oricare din următoarele situații: (a) persoana vizată şi-a dat consimțământul explicit pentru prelucrarea acestor date, cu excepția cazurilor în care legislația statului membru prevede ca interdicția prevăzută la alineatul 1 să nu poată fi ridicată prin consimțământul persoanei vizate;”*

a) În consecință, o confirmare a prelucrării de date confidențiale poate fi constituită de către **consimțământul** persoanei vizate[10]. După cum s-a menționat în documentele de lucru anterioare WP 12[11] şi WP 114[12] ale Grupului de lucru, un argument important este că, pentru a fi valabil, consimțământul – oricare ar fi circumstanțele în care acesta este exprimat – trebuie să fie o“*manifestare de voință, liberă, specifică şi informată a persoanei vizate*”, conform definiției din articolul 2 alineatul (h) din directivă.

> aa) Consimțământul trebuie să fie dat de bună voie: Consimțământul de „bună voie” presupune o decizie voluntară a unei persoane aflate în deplinătatea facultăților mentale, în lipsa unor constrângeri de orice fel, fie sociale, financiare, psihologice sau de altă natură. Orice consimțământ dat ca urmare a amenințării întreruperii tratamentului sau a tratamentului de calitate inferioară într-o circumstanță medicală nu

[10] Acordul de a fi supus unui anumit tratament medical nu presupune “consimțământul” automat în sensul articolului 2 litera (h) pentru prelucrare (în special dezvăluire sau transfer) a datelor cu caracter personal colectate în timpul unui asemenea tratament.

[11] Grupul de lucru pentru articolul 29 “Document de lucru: Transferul de date cu caracter personal către terțe țări: Aplicarea articolelor 25 şi 26 din Directiva UE privind protecția datelor” (WP 12, 24 iulie 1998).

[12] Grupul de lucru pentru articolul 29 “Document de lucru privind o interpretare comună a articolului 26(1) din Directiva 95/46/CE din 24 octombrie 1995” (WP 114, 25 noiembrie 2005).

poate fi considerat „de bună voie”. Consimțământul dat de către o persoană vizată căruia nu i s-a oferit şansa unei opțiuni autentice sau *care a fost pus în fața faptului împlinit* nu poate fi considerat ca fiind valabil.

Grupul de lucru pentru articolul 29 consideră că, în cazul în care un cadru medical trebuie să prelucreze date cu caracter personal în sistemul DES ca o urmare necesară şi inevitabilă a actului medical, justificarea acestei prelucrări prin primirea acordului este falsă. Utilitatea acordului trebuie limitată la cazurile în care subiectul individual al datelor beneficiază de mai multe opțiuni reale şi poate ulterior să-şi retragă acordul fără a suferi neajunsuri.[13]

bb) Consimțământul trebuie să fie specific: Consimțământul „specific” trebuie să privească o situație bine definită, concretă, unde este avută în vedere prelucrarea datelor medicale. În consecință, un ‘acord general’ al persoanei vizate privind colectarea datelor sale medicale pentru un DES şi al transferului ulterior al acestor date medicale din trecut şi viitor către cadre medicale implicate în tratament nu constituie un consimțământ în sensul articolului 2 litera (h) din directivă.

cc) Consimțământul trebuie să fie în cunoştință de cauză: Consimțământ „în cunoştință de cauză” se referă la un consimțământ al persoanei vizate întemeiat pe judecarea şi înțelegerea faptelor şi implicațiilor unei decizii. Individul în cauză trebuie să primească, într-o manieră clară şi inteligibilă, date exacte şi complete despre toate aspectele relevante, în special despre cele menționate în articolele 10 şi 11 ale directivei, precum natura datelor prelucrate, scopul prelucrării, destinatarii posibilelor transferuri şi drepturile persoanei vizate. Aceasta include şi cunoaşterea consecințelor în cazul refuzului pentru prelucrarea în cauză.

b) În contrast cu prevederile articolului 7 din directivă, consimțământul în cazul datelor confidențiale cu caracter personal şi, în consecință, într-un DES, trebuie să fie **explicit**. Soluțiile care implică o renunțare nu întrunesc condițiile de a fi „explicite”. În conformitate cu definiția generală prin care consimțământul presupune o declarație de intenții, atributul de explicit trebuie să se refere, în particular, la **confidențialitatea datelor**. Persoana vizată trebuie să fie conştientă că renunță la protecția specială. Consimțământul scris nu este totuşi necesar.

c) Grupul de lucru pentru articolul 29 a observat că, în unele cazuri, obținerea consimțământului poate fi dificilă din cauza unor probleme practice, mai ales în situațiile în care nu există un contact direct între managerul de date şi persoanele vizate. Oricare ar fi aceste dificultăți, **managerul de date** trebuie să demonstreze în toate cazurile că a obținut, în primul rând, consimțământul explicit al fiecărui subiect al datelor şi, în al doilea rând, că acest consimțământ explicit a fost dat în temeiul unor date exacte.

d) Din nou în contradicție cu articolul 7, articolul 8 alineatul (2) litera (a) recunoaşte că pot exista cazuri de prelucrare a datelor confidențiale în care **nici măcar consimțământul explicit** al persoanei vizate nu poate anula interdicția prelucrării: statele membre au libertatea de a reglementa astfel de cazuri în detaliu.

---

13 A se vedea şi “Avizul 8/2001 privind prelucrarea datelor cu caracter personal în contextul ocupării unui loc de muncă” (WP 84, secțiunea 10).

5. Articolul 8 alineatul (2) litera (c): "interesele vitale ale persoanei vizate"

Prelucrarea datelor confidențiale cu caracter personal poate avea loc în cazul existenței necesității protejării intereselor vitale ale persoanei vizate sau ale unei alte persoane în cazul în care persoana vizată nu are capacitatea fizică sau legală de a-şi manifesta consimțământul.

Prelucrarea trebuie să aibă legătură cu interesele individuale esențiale ale unei alte persoane şi trebuie – în context medical – să fie necesară pentru un tratament de importanță crucială într-o situație când persoana vizată nu are capacitatea de a-şi exprima intențiile. În mod corespunzător, această excepție poate fi aplicată exclusiv într-un mic număr de tratamente şi nu poate fi invocată în nici o privință pentru a justifica prelucrarea datelor medicale cu caracter personal pentru alte scopuri în afara tratamentului persoanei vizate precum, de exemplu, desfăşurarea de cercetări medicale care nu vor oferi rezultate decât într-o perioadă viitoare.[14]

> De exemplu: se presupune că o persoană vizată şi-a pierdut cunoştința după un accident şi nu îşi poate da consimțământul pentru aflarea alergiilor cunoscute. În contextul sistemelor DES, această prevedere va permite accesul la datele stocate în DES de către un cadru medical pentru a extrage date despre alergiile cunoscute ale persoanei vizate, acestea putând fi decisive în alegerea unui anumit tratament.

6. Articolul 8 alineatul (3): „prelucrarea datelor (medicale) de către cadrele medicale"

Articolul 8 alineatul (3) permite prelucrarea datelor confidențiale cu caracter personal dacă sunt îndeplinite trei condiții cumulative: prelucrarea datelor confidențiale cu caracter personal trebuie să fie *„necesară", iar această prelucrare are loc "în scopuri legate de medicina preventivă, de stabilire a diagnosticelor medicale, de administrare a unor îngrijiri sau tratamente ori de gestionare a serviciilor de sănătate"* iar datele personale în chestiune *"sunt prelucrate de către un cadru medical supus, în conformitate cu dreptul intern ori cu normele stabilite de autoritățile naționale competente, secretului profesional, sau de altă persoană supusă, de asemenea, unei obligații echivalente în ceea ce priveşte secretul"*.

a) Această derogare acoperă exclusiv prelucrarea datelor cu caracter personal pentru **scopul specific** de a furniza servicii medicale de natură preventivă, de diagnostic sau post-tratament, şi în scopul gestionării de servicii medicale precum facturare, contabilitate sau statistică.

Nu este acoperită prelucrarea ulterioară care nu este necesară pentru furnizarea directă de servicii precum cercetarea medicală, rambursarea ulterioară a costurilor de către un fond de asigurări de sănătate sau de urmărire a revendicărilor financiare. În afara sferei de aplicare a articolului 8 alineatul (3) sunt şi alte operațiuni de prelucrare în sectoare precum sănătatea publică şi protecția socială, mai ales pentru a asigura calitatea şi eficiența financiară a procedurilor utilizate pentru reglementarea revendicărilor pentru acordarea de beneficii şi serviciilor în sistemul de asigurări de sănătate, aşa cum sunt prezentate în expunerea de motive nr. 34 din directivă ca exemple pentru invocarea articolului 8 alineatul (4).

b) În afară de aceasta, prelucrarea datelor cu caracter personal în temeiul articolului 8 alineatul (3) trebuie să fie „**obligatorie**" pentru obiectivele specifice menționate la litera a). Grupul de lucru subliniază că, într-un context DES, aceasta presupune că orice includere de date cu caracter personal într-un DES va trebui să fie bine justificată; simpla „utilitate" a prezenței unor asemenea date cu caracter personal într-un DES nu va fi suficientă.

---

[14] Pentru o interpretare a dispoziției similare conținută în articolul 26 alineatul (1) litera (e) privind transferul de date în afara UE, a se vedea "Documentul de lucru privind o interpretare comună a articolului 26 alineatul (1) din Directiva 95/46/CE din 24 octombrie 1995", WP 114, (25 noiembrie 2005).

c) A treia condiție din articolul 8 alineatul (3) este aceea ca prelucrarea datelor medicale cu caracter personal să fie îndeplinită de către personal medical sau alt tip de personal supus obligației de a păstra **secretul profesional (medical) sau o obligație echivalentă de confidențialitate.**

> Obligația etică de confidențialitate a profesiei medicale a fost expusă pentru prima dată în "Jurământul lui Hipocrate"[15], fiind apoi afirmată de către Declarația Asociației Medicale Mondiale de la Geneva (1948). Ea protejează datele colectate de către un cadru medical în cursul tratamentului unui pacient. Utilizarea acestor date este permisă doar în limitele contractului de tratament. Această relație de confidențialitate exclude toate terțele părți, inclusiv alte cadre medicale, dacă pacientul nu şi-a manifestat consimțământul pentru transmiterea datelor sale sau în cazurile prevăzute special de către lege.

Grupul de lucru arată că obligația specială de a păstra secretul profesional trebuie să fie conținută în legislația națională a statelor membre sau a organismelor profesionale naționale competente cu puterea de a adopta reguli obligatorii ale profesiei. Aceste reguli naționale privind secretul profesional trebuie să includă şi sancțiunile corespunzătoare în caz de încălcare a lor.

Conform directivei, dacă există necesitatea ca personalul non-medical să prelucreze date confidențiale cu caracter personal, acesta trebuie să fie supus regulilor obligatorii care asigură cel puțin un nivel echivalent de confidențialitate şi protecție. În special, aceste reguli trebuie să conțină obligația ca datele să fie utilizate exclusiv în sensul menționat în articolul 8 alineatul (3).

Cadrele medicale cu responsabilitate directă pentru tratamentul pacienților au, în general, obligația legală de a păstra documentația privind tratamentul medical (măsuri, rețete etc.) la dosarul pacienților. Conform numeroaselor dispoziții legale în vigoare privind obligativitatea păstrării secretului profesional de către cadrele medicale, reținerea şi utilizarea dosarelor pacienților este limitată în mod tradițional la relația directă între pacient şi cadrul medical/instituția medicală la care pacientul a apelat.

d) Deoarece articolul 8 alineatul (3) din directivă reprezintă o excepție de la interdicția generală de prelucrare a datelor confidențiale, această excepție trebuie interpretată într-o manieră strictă.

e) Dacă există îndoiala că articolul 8 alineatul (3) din directiva poate constitui baza legală *unică* pentru prelucrarea datelor personale într-un sistem DES, Grupul de lucru pentru articolul 29 consideră că articolul 8 alineatul (3) se poate referi exclusiv la prelucrarea datelor medicale numai în scopurile medicale şi de tratament menționate, şi numai în condițiile în care prelucrarea este „solicitată" şi îndeplinită de către un cadru medical sau de către altă persoană supusă obligației de a păstra un secret profesional sau echivalent. Dacă prelucrarea datelor personale în DES depăşeşte în orice privință aceste scopuri sau nu întruneşte condițiile menționate, articolul 8 alineatul (3) nu poate fi invocat ca bază legală unică pentru prelucrarea acelor date cu caracter personal.

Cu toate acestea, chiar dacă toate aceste condiții ar fi întrunite, Grupul de lucru pentru articolul 29 trebuie să afirme că sistemele DES contribuie la apariția unui nou risc, care necesită noi măsuri de protecție în contramăsură: sistemele DES furnizează acces direct la o compilație a documentației existente privind tratamentul medical al unor anumite persoane, din diferite surse (de ex. spitale, cadre medicale) pe parcursul întregii vieți. Astfel de sisteme

---

[15] *"Tot ce pot să aflu în timpul exercitării profesiunii mele sau în relațiile zilnice cu oamenii ce nu ar trebui răspândit, voi păstra ca taină şi nu voi dezvălui niciodată."* (Sursă: http://en.wikipedia.org/wiki/Hippocratic_Oath).

DES depăşesc, prin urmare, frontierele tradiționale ale relației directe între pacientul individual şi cadrul medical sau instituția: Păstrarea datelor medicale într-un DES depăşeşte metodele tradiționale de păstrare şi utilizare a documentației privind pacienții. Din punct de vedere tehnic, punctele de acces multiple dintr-o rețea deschisă precum internetul cresc riscul interceptării datelor pacientului. Menținerea standardului legal de confidențialitate adecvat într-un mediu tradițional se poate dovedi insuficient pentru protejarea intereselor unui pacient după ce dosarul electronic de sănătate a devenit disponibil pe Internet. Sistemele DES dezvoltate complet tind astfel să ofere şi să faciliteze accesul la datele medicale şi datele confidențiale cu caracter personal. Sistemele DES întâmpină dificultăți în a se asigura că doar cadrele medicale autorizate primesc acces la date, în scopuri legitime, privind tratamentul persoanei vizate. Acestea conferă prelucrării datelor o dimensiune mai complexă, cu implicații directe pentru drepturile indivizilor. În consecință, un sistem DES trebuie să fie considerat o nouă situație de risc pentru protecția datelor confidențiale cu caracter personal.

Principala şi tradițională măsură de protecție descrisă de art. 8 alineatul (3) – cu excepția limitării scopului şi obligației de strictă necesitate – este obligația cadrelor medicale de a păstra confidențialitatea datelor medicale ale propriilor pacienți. Aceasta poate să nu mai fie aplicabilă într-un mediu DES, deoarece unul din scopurile DES este de a furniza accesul la documentația medicală în scopuri de tratament acelor cadre care nu au contribuit la tratamentele anterioare documentate într-un dosar medical.

Prin urmare, Grupul de lucru pentru articolul 29 nu este convins că, chiar dacă articolul 8 alineatul (3) este utilizat ca justificare pentru prelucrare, respectarea obligației secretului profesional oferă o protecție suficientă într-un sistem DES. O nouă situație de risc reclamă măsuri adiționale de protecție mai noi decât cele descrise în articolul 8 alineatul (3), în scopul asigurării unei protecții adecvate a datelor cu caracter personal în context DES.

7. Articolul 8 alineatul (4): derogările de interes public important

Unele dintre dispozițiile directivei conțin un grad înalt de flexibilitate, pentru a garanta un echilibru corespunzător între protecția drepturilor persoanei vizate, pe de o parte, şi eventualelor interese legitime ale managerilor de date, terților părți şi interesului public, pe de altă parte.

Articolul 8 alineatul (4) din directivă permite statelor membre să stabilească şi alte derogări de la interdicția prelucrării categoriilor de date confidențiale:

> *„Sub rezerva unor garanții corespunzătoare, statele membre pot prevedea, pentru un motiv de interes public important, derogări suplimentare față de cele prevăzute în alineatul 2, fie în legislația internă, fie prin decizia autorității de supraveghere.”*
>
> Expunerea de motive nr. 34 afirmă:
>
> *(34) „Întrucât statele membre trebuie, de asemenea, să fie autorizate să deroge de la interdicția privind prelucrarea categoriilor de date sensibile atunci când aceasta se justifică din motive de interes public important în domenii cum ar fi sănătatea publică şi protecția socială – în special în scopul asigurării calității şi rentabilității în ceea ce priveşte procedurile folosite pentru soluționarea cererilor de prestații şi servicii în sistemul asigurărilor de sănătate – cercetarea ştiințifică şi statistica guvernamentală; întrucât este totuşi de datoria lor să prevadă garanții specifice şi corespunzătoare în scopul protejării drepturilor fundamentale şi vieții private a indivizilor;”*

a) În consecință, dacă un stat membru intenționează să utilizeze această posibilitate, derogarea trebuie să fie conținută într-o dispoziție legală sau decizie a autorității de supraveghere (**bază legală specială**).

b) O asemenea prelucrare a datelor confidențiale cu caracter personal trebuie justificată prin motive de **interes public important**. Expunerea de motive nr. 34 din directivă oferă exemple de domenii care pot conține cazuri de „interes public important". Acestea includ domeniile sănătății publice şi asigurărilor sociale, pentru a asigura calitatea şi eficiența financiară a procedurilor utilizate pentru soluționarea cererilor de prestații şi servicii în sistemul asigurărilor de sănătate.

Interesul public important trebuie prezentat de către statul membru pentru fiecare caz în întreaga sferă a prelucrării derogate, iar prelucrarea trebuie să fie necesară din perspectiva acelui interes public important. Orice astfel de măsură trebuie să fie proporțională, semnificând că nu trebuie să existe alte măsuri mai puțin limitative.

În plus, orice încălcare a dreptului la viață privată şi de familie, pentru a fi legitimă, trebuie să respecte articolul 8 din Convenția europeană a drepturilor omului şi trebuie citită în lumina jurisprudenței de la Strasbourg: trebuie să fie "*conform legii*" şi să fie "*necesară într-o societate democratică*" pentru un scop de interes public. Jurisprudența de la Strasbourg a afirmat în mod repetat că legea care justifică încălcarea „*trebuie să indice sfera puterilor discreționare oferite autorităților competente şi modul de exercitare a acestora cu suficientă claritate, având în vedere scopul legitim al măsurii în chestiune, pentru a proteja corespunzător individul împotriva abuzurilor*".

c) Statele membre au obligația să furnizeze **măsuri de protecție specifice şi adecvate** pentru a proteja drepturile fundamentale şi confidențialitatea indivizilor în acel context.

d) Orice utilizare a articolului 8 alineatul (4) de către un stat membru trebuie **notificată Comisiei** conform articolului 8 alineatul (6) din directivă.

În contextul DES, Grupul de lucru pentru articolul 29 observă că argumentele favorabile introducerii sistemelor DES (vezi I., mai sus) pot reprezenta "interes public substanțial". În unele state membre, „dreptul de protecție a sănătății" este considerat sacru de către constituție. Aceasta subliniază importanța atribuită tuturor mijloacelor adecvate pentru asigurarea „protecției sănătății". Un sistem DES într-un asemenea cadru legal se va baza cu siguranță pe „interes public important" deoarece este un instrument dedicat fundamental oferirii de asistență medicală adecvată pacienților.

Articolul 8 alineatul (4) din directivă ar putea, prin urmare, să constituie bază legală pentru sistemele DES dacă toate condițiile menționate aici sunt respectate. Trebuie oferite, în particular, mijloace de protecție adecvate pentru protecția datelor cu caracter personal dintr-un sistem DES.

Grupul de lucru dorește să trateze asemenea mijloace de protecție posibile şi cadrul legal adecvat pentru sistemele DES în următoarea secțiune.

III. Considerații asupra unui cadrul legal adecvat pentru sistemele DES

Grupul de lucru pentru articolul 29 oferă mai jos detalii despre acele subiecte în cazul cărora pot fi invocate mijloacele de protecție specială[16] din cadrul sistemelor DES pentru garantarea

[16] Condițiile generale prevăzute în Directiva 95/46/CE pentru prelucrarea datelor cu caracter personal conform legii nu sunt repetate în această parte a documentului deoarece ele se aplică oricum. Acest document

drepturilor pacienților de a le fi protejate datele. Având în vedere impactul sistemelor DES şi a nevoii de transparență a unor asemenea sisteme, mijlocele de protecție trebuie prezentate, în mod preferabil, într-un cadrul legal special şi complet.

1. Respectarea autodeterminării

Chiar dacă un sistem DES nu este fundamentat pe acord ca bază legală (articolul 8 alineatul (2)), autodeterminarea pacientului privind timpul şi modul în care sunt utilizate datele sale trebuie să aibă un rol semnificativ ca mijloc major de protecție.[17]

a) Funcționalitatea „consimțământului" în contextul mijloacelor de protecție adecvate este diferită de cea a „consimțământului" din articolul 8 alineatul (2) din directivă şi, prin urmare, nu trebuie să îndeplinească toate condițiile din articolul 8 alineatul (2): de ex. întrucât **consimțământul ca bază legală** pentru prelucrarea datelor medicale ar trebui să fie întotdeauna „explicit" conform articolului 8 alineatul (2), **consimțământul ca mijloc de protecție** nu trebuie oferit în mod necesar sub forma participării – posibilitatea de afirmare a autodeterminării ar putea – în funcție de situație – să se manifeste sub forma unei neparticipări/ a unui drept de a refuza.

b) Având în vedere potențialul negativ variat al diferitelor tipuri de date medicale, situațiile categoriilor de utilizare trebuie diferențiate în funcție de **diferite situații de exercitare a autodeterminării**:

Dispozițiile legale de înființare a unui sistem DES trebuie să includă reglementarea prin care introducerea de date într-un DES sau accesarea unor astfel de date trebuie să fie guvernată de un sistem cumulativ de condiții de „participare" (în special în cazul prelucrărilor de date foarte sensibile precum date psihiatrice, despre avorturi etc.[18]) şi posibilități de „neparticipare" pentru date mai puțin sensibile.[19] Aceasta poate garanta gradul de protecție necesară, pe de o parte, şi operabilitatea şi flexibilitatea, pe de altă parte.

c) În principiu, **un pacient ar trebui să aibă întotdeauna posibilitatea să prevină dezvăluirea** datelor sale medicale, dobândite de către un cadru medical în timpul tratamentului, către alte cadre medicale, dacă doreşte acest lucru.

Trebuie acordată atenție modului în care poate fi gestionată limitarea accesului la informație într-un DES: Dacă limitarea ar trebui să fie disimulată pentru a nu fi detectabilă sau dacă, în anumite cazuri, ar trebui să fie transmisă o notă prin care se recunoaşte existența unor date suplimentare, dar care sunt disponibile doar în condiții speciale.

d) Plecând de la premisa că nimeni nu poate fi obligat să participe într-un sistem DES, problema **opțiunii de retragere completă dintr-un sistem DES** trebuie să fie inclusă în dispozițiile legale de înființare a unui sistem DES. Trebuie prevăzute reguli în cazurile în care aceasta impune o obligație de distrugere a datelor sau doar de limitare a accesului la datele din

---

discută doar condițiile suplimentare specifice pentru prelucrarea datelor cu caracter medical în sistemele DES, care se pot dovedi necesare pentru a contrabalansa riscul la adresa confidențialității pe care îl implică sistemele DES.

[17] În unele jurisdicții nu există doar un drept fundamental la protecția datelor, dar şi un drept constituțional la protecția optimă a sănătății: ca urmare a existenței acestei obligații de asigurare a unui tratament optim, unele state membre au atribuit cadrelor medicale acces privilegiat la datele disponibile în sistemul DES. Această realitate poate fi acceptabilă atât timp cât se obține un echilibru necesar insistând asupra altor mijloace de protecție, precum reglementările detaliate privind circumstanțele accesului conform legii şi consecințele – severe – în cazurile de folosire abuzivă a drepturilor de acces etc.

[18] Pot fi utilizate facilități speciale precum "plicuri sigilate", care nu pot fi deschise fără cooperarea persoanei vizate.

[19] Soluțiile de neparticipare vor necesita totuşi o informare corespunzătoare a pacientului pentru a fi eficiente ca "mijloace de protecție adecvate".

sistemul DES; persoanele vizate pot primi dreptul de a-şi exprima opțiunea în această privință.

2. Identificarea şi autentificarea pacienților şi cadrelor medicale

a) Identificarea corectă[20] a pacienților în sistemele DES prezintă o importanță crucială. Utilizarea unor date ale altor persoane ca urmare a unei identificări incorecte a pacientului poate avea consecințe negative în majoritatea cazurilor.

Cardurile de sănătate pe platformă de carduri inteligente pot contribui în mod semnificativ la identificarea electronică corectă a pacienților, precum şi la **autentificarea lor,[21] dacă aceştia doresc să-şi acceseze propriile date DES.**

b) În plus, confidențialitatea datelor medicale presupune interzicerea accesului pentru persoanele neautorizate. Controlul eficient al accesului depinde de o identificare şi autentificare corectă[22]. Aceasta presupune necesitatea **identificării unice şi a autentificării corecte a utilizatorilor**.[23]

Deoarece unul dintre principalele avantaje ale sistemelor DES este capacitatea lor de a fi accesate prin mijloace electronice indiferent de oră şi locație, trebuie puse la punct metode de identificare electronică şi autentificare eficiente. Autentificarea prin intermediul semnăturii electronice – furnizată utilizatorilor autorizați împreună cu mijloace de identificare oficiale de ex. pe carduri inteligente speciale – trebuie luată în considerare cel puțin ca perspectivă îndepărtată pentru a fi evitate riscurile cunoscute ale autentificării prin parolă.

Pentru cadrele medicale va fi necesară dezvoltarea unui sistem de identificare şi autentificare, care va verifica nu doar identitatea, ci şi **calitatea în care un cadru medical acționează în mediul electronic**, de ex. ca psihiatru sau asistent medical.

3. Autorizarea accesării DES pentru citirea şi introducerea de date în DES

a) Mijloace de protecție generale referitoare la acces:

Datele din sistemele DES sunt constituite din dosare medicale confidențiale. Astfel, **principiul fundamental** care guvernează accesul la un DES trebuie să fie acela că – în afară de pacient **– doar** acele **cadre medicale**/persoane autorizate de instituții medicale, **care participă activ** la **tratamentul pacientului pot primi dreptul de acces**. Trebuie să existe o relație profesională medicală între pacient şi cadrul medical care solicită accesul la dosarul DES al acestuia.

Se conturează ca necesară şi reglementarea categoriilor de cadre medicale/instituții şi a nivelului la care aceştia vor accesa datele DES (medici practicanți, medici din spitale, farmaciști, asistenți medicali, chiropracticieni?, psihologi?, consilieri familiali? etc.).

Protecția datelor mai poate fi ameliorată cu ajutorul **drepturilor de acces modulare**, prin formarea de categorii de date medicale într-un sistem DES, cu consecința limitării accesului

---

[20] Noțiunea de "Identificare" presupune că o persoană este caracterizată de identificatori precum nume, dată de naştere, adresă etc.; în prezentul context, această descriere va trebui susținută în mod oficial de către un certificat de naştere, un paşaport sau un card de sănătate etc.

[21] "Autentificare" reprezintă dovada faptului că o persoană care îşi declină o anumită identitate este cu adevărat acea persoană. Aceasta se obține prin prezentarea unui act oficial de identitate conținând o fotografie (de ex. un paşaport), sau – în mediu electronic – prin utilizarea unei semnături electronice.

[22] "Identificarea corectă" nu trebuie să utilizeze numerele de identificare, sunt folosite pe scară largă în alte contexte, fără mijloace de protecție specifice, pentru a evita interconectabilitatea facilă (vezi articolul 8(7) al directivei.

[23] În Franța, primele experimente cu DES iau în considerare crearea unui identificator specific; nu se ştie încă dacă acest sistem va fi menținut în versiunea finală a DES.

în favoarea unor categorii specifice de cadre medicale/instituții[24]. Posibilele avantaje ale variantei modulare a DES vor fi discutate în detaliu la punctul 6.

b) Mijloace de protecție specială cu implicarea pacientului:

Dacă există cadrul şi posibilitatea – şi dacă pacientul este prezent şi conştient – **pacientul poate împiedica accesul la datele sale DES dacă doreşte astfel**. Aceasta presupune informarea sa prealabilă în privința persoanelor şi motivelor care reclamă accesul la datele sale şi despre posibilele consecințe ale refuzului de a permite accesul. Trebuie puse la punct proceduri care vor preîntâmpina presiunile asupra pacientului pentru obținerea acordului său de acces la propriile date.

Când este necesară **dovada acordului pacientului** pentru accesarea datelor sale DES, este indispensabilă utilizarea unor instrumente adecvate pentru obținerea unor asemenea dovezi, precum verificarea electronică a simbolului pacientului sau – dacă astfel de instrumente sunt disponibile pe scară largă – semnătura electronică a pacientului etc. Prezentarea unor asemenea dovezi trebuie să fie stocată electronic pentru posibilele verificări ulterioare.

Trebuie să apară prevederi referitoare la cazurile când persoana vizată solicită ca anumite date să nu fie introduse în propriul dosar. O modalitate de a aborda astfel de situații poate fi utilizarea "plicurilor sigilate" care nu pot fi deschise fără acordul explicit al persoanei vizate.

c) Accesul persoanelor vizate la propriile date DES:

Acordarea **accesului direct (electronic) pentru citirea** DES către pacienți este o problemă de posibilitate medicală. Dreptul de acces pentru protecția datelor de ex. conform articolului 12 din Directiva 95/46/CE nu presupune întotdeauna în mod necesar accesul *direct*. Accesul direct poate totuşi să contribuie considerabil la dobândirea încrederii într-un sistem DES. Din punctul de vedere al protejării datelor, o condiție prealabilă pentru furnizarea accesului direct va fi identificarea electronică securizată şi autentificarea, în scopul de a preveni accesul persoanelor neautorizate.

Întrebarea dacă **pacienții** înşişi pot **introduce date în propriul DES** sau dacă acestea trebuie să fie introduse de către un cadru medical trebuie să primească, de asemenea, un răspuns în cadrul dispozițiilor de înființare ale unui sistem. O transparență corectă privind urmărirea activității, care să dezvăluie identitatea autorului introducerii datelor într-un dosar DES, va rezolva problemele responsabilității pentru corectitudine. Se mai consideră că transparența va limita accesul pentru introducerea de date la un modul special dintr-un dosar DES.

În acest context, trebuie avute în vedere capacitățile şi nevoile speciale ale bolnavilor cronici, persoanelor în vârstă, precum şi ale persoanelor cu handicap sau invaliditate.

4. Utilizarea DES în alte scopuri

Acceptarea sistemelor DES de către cetățeni va depinde de **încrederea lor în confidențialitatea sistemului.**

Motivul accesului legitim la datele dintr-un sistem DES trebuie să corespundă scopului principal al unui sistem DES de a garanta tratament medical de succes prin intermediul datelor corecte. **Grupul de lucru consideră că accesarea datelor medicale într-un DES în alte scopuri decât cele menționate în articolul 8 alineatul (3) ar trebui să fie interzise în principiu.**

[24] De exemplu, accesul la datele despre tratamentul psihiatric pot fi limitate la un prim nivel pentru medicii psihiatri; sau un modul privind medicația specială poate fi pus la dispoziția farmaciştilor, care nu au acces la celelalte părți ale unui sistem DES.

De exemplu, aceasta va exclude accesul la DES al cadrelor medicale care acționează ca experți pentru terțe părți: de ex. pentru companii private de asigurări, în litigii, pentru acordarea de asistență la pensionare, pentru angajatorii persoanei vizate etc. În plus, legislația disciplinară aplicabilă în cazul cadrelor medicale trebuie concepută astfel încât să descurajeze în mod efectiv încălcarea acestor reglementări.

Trebuie adoptate măsuri speciale pentru a preveni ca pacienții să fie determinați în mod ilegal să-şi dezvăluie datele DES, de ex. 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 conform legii protecției datelor. Pot fi aplicate şi mijloace tehnice de ex. solicitări speciale pentru imprimarea integrală a unor date dintr-un DES etc.

Prelucrarea datelor DES în scopul **cercetării medicale ştiințifice şi al statisticii guvernamentale** poate fi considerată o excepție de la regula de mai sus**,** dacă toate aceste excepții respectă prevederile directivei (a se vedea articolul 8 alineatul (4) şi a expunerii de motive nr. 34): acestea trebuie, prin urmare, să fie prevăzute de lege pentru scopuri predeterminate şi specifice, conform condițiilor speciale de garantare a proporționalității („mijloace de protecție specifice şi adecvate") pentru a proteja drepturile fundamentale şi viața privată a persoanelor.

Mai mult, oricând este realizabil şi posibil, datele din sistemele DES ar trebui folosite în alte scopuri (de ex. statistică sau evaluarea calității) doar sub formă anonimă sau, cel puțin, la adăpostul unui pseudonim sigur[25].

5. Structura de organizare a unui sistem DES

În contextul discutării diferitelor alternative de organizare pentru stocarea de date într-un sistem DES, următoarele alternative principale sunt menționate în mod obişnuit:

- DES ca sistem care oferă acces la dosarele medicale aflate în posesia cadrului medical, care are obligația de a păstra istoricul tratamentului pacienților săi – aceasta fiind numită **"stocare descentralizată",** sau
- DES ca sistem uniform de stocare, unde cadrele medicale trebuie să-şi transfere documentația; aceasta este frecvent numită **"stocare centralizată";**
- o a treia alternativă poate fi posibilitatea ca persoana vizată să fie "stăpânul" propriilor date medicale, oferindu-i-se posibilitatea **stocării datelor medicale ale pacientului sub formă de serviciu electronic aflat sub controlul pacientului**, având, eventual, puterea de a selecta datele care pot fi incluse în DES.[26]

a) Întrucât a treia alternativă **(stocarea sub controlul persoanei vizate)** pare a fi cea mai bună soluție din punct de vedere al autodeterminării, calitatea unei asemenea documentații poate ridica probleme din punctul de vedere al exactității şi exhaustivității dacă persoana vizată decide în exclusivitate care sunt datele care urmează a fi stocate în propriul DES şi nici o metodă de corecție medicală nu este integrată în sistem.

b) În cazul unui model de **stocare "descentralizată"**, care devine sistem doar prin crearea mijloacelor de căutare corespunzătoare, structura existentă a documentației de date medicale

[25] Pseudonimul conține identificatori (precum nume şi date de naştere etc.) transpuşi sub o nouă denumire, preferabil prin encriptare, astfel încât destinatarul informației să îi fie în imposibilitatea de a identifica persoana vizată.

[26] Modelul impus în practică este cel francez. Acei furnizori de servicii sunt numiți gazde ("hébergeurs") şi poziția lor este reglementată printr-un decret care a fost supus avizului prealabil al CNIL. Decretul este complex şi vizează problemele de acreditare ale acelor furnizori de servicii şi a securității sistemului.

de la diferiți furnizori de servicii medicale va rămâne neschimbată. Măsura în care datele unui pacient pot fi localizate în acest sistem depinde de calitatea sistemului de căutare.

În acest model de organizare, **cadrul/instituția medicală rămâne „managerul”** fişierului (mai exact: a acelei părți a dosarului DES pe care a creat-o). Luând în considerare arhitectura complexă a acestui model, poate fi necesară numirea unui organism centralizat în scopul controlării şi monitorizării întregului sistem, dar şi pentru asigurarea compatibilității protecției datelor din operarea sistemului. Se poate dovedi util ca persoanele vizate să prezinte toate problemele privind protecția datelor unui organism centralizat, în loc de a fi nevoiți să identifice unul dintre multitudinea de manageri.

c) Principalul avantaj al sistemului de **stocare “centralizată”** poate fi gradul înalt de securitate şi disponibilitate (acces 24/24), care nu poate fi asigurat la fel de uşor dacă un sistem DES depăşeşte granița spitalelor. Va exista un singur manager pentru întregul sistem, separat de cadrele/instituțiile medicale care şi-au înaintat documentația (parțial sau în întregime) către sistemul centralizat.

În privința protejării datelor, pot apare obiecții la adresa unui astfel de sistem privind posibilitățile numeroase de utilizare abuzivă a stocării centralizate a datelor. Proceduri speciale şi măsuri de securitate (de ex. stocare encriptată) pot fi prevăzute pentru a coborî riscurile de securitate ale datelor stocate centralizat, cel puțin într-o măsură considerabilă. Cu toate acestea, răspunderea pentru confidențialitatea sistemului nu mai revine cadrelor medicale, ceea ce poate afecta încrederea pacienților într-un astfel de sistem.

Măsura în care pacientul poate influența conținutul şi dezvăluirea dosarului său DES va depinde în ambele cazuri – stocare descentralizată şi stocare centralizată – de modul de funcționare a sistemului (vezi punctul 3 b).

6. Categorii de date stocate în DES şi modul de prezentare a acestora

Obiectivul “sistemului DES” este de a colecta toate datele medicale relevante pentru starea de sănătate pe termen lung a unei anumite persoane, astfel încât, în cazul unui viitor tratament, datele complete şi relevante vor fi disponibile, iar pacienții vor beneficia de un tratament eficient.

Grupul de lucru consideră că acest aspect poate provoca apariția următoarelor probleme importante:

a) “Exhaustivitatea” unui dosar medical nu este posibilă din punct de vedere practic şi nici dezirabilă: **Doar informația *relevantă* trebuie introdusă într-un DES**. Unul dintre cele mai dificile aspecte din timpul înființării unui sistem DES va fi, prin urmare, de a decide care categorii de date medicale vor fi colectate într-un DES şi pentru ce perioadă de timp vor fi stocate[27]. Întrucât acest aspect va fi lămurit în principal de către experți medicali, mai are şi o dimensiune a protecției datelor: Conform principiilor relevanței şi proporționalității colectării de date, fiecare compilație de date trebuie să fie limitată la acele date care sunt relevante şi nu depăşesc scopul definit al prelucrării (articolul 6 alineatul (1) litera (c) din directivă). Legitimitatea sistemelor DES va depinde, prin urmare, de alegerea adecvată a categoriilor de date „corecte” şi a perioadei de timp „corecte” pentru stocarea datelor într-un DES.

b) În privința prezentării de date în cadrul DES: Faptul că este posibilă distingerea diferitelor categorii de date medicale care necesită diferite grade de confidențialitate sugerează utilitatea creării unor diferite **module de date** în cadrul unui sistem DES cu cerințe

[27] Există categorii de date considerate importante pentru întreaga durată a vieții pacientului (de ex.. alergii) dar şi date care sunt extrem de importante doar pentru o perioadă scurtă de timp, cum ar fi de ex. incompatibilitățile de tratament.

diferite de acces: Un „modul de date despre vaccinări" ar trebui să fie accesibil în orice moment pentru persoana vizată, putând fi accesibil şi pentru un personal destul de numeros din cadrul serviciilor medicale; un „modul de date despre medicație" ar putea fi accesat de către farmacişti dacă pacientul este de acord[28]; un „modul de date de urgență" ar putea conține mijloace tehnice speciale pentru acces etc. Înființarea unor module pentru „sisteme de reamintire" poate fi utilă; ele vor avea scopul de a reaminti în mod automat unui pacient vaccinurile, consulturile medicale şi examinările post-tratament care urmează.

Anumite date confidențiale pot fi protejate mai eficient prin stocarea în module separate, având condiții stricte de acces. Acestea pot fi date despre tratamentele psihiatrice, contaminarea HIV sau avorturi. În loc de a exclude astfel de date dintr-un DES – ceea ce ar putea avea consecințe negative pentru un viitor tratament – restricții speciale pentru accesul la aceste date DES trebuie să fie integrate în sistem, inclusiv acordul explicit al pacientului şi mijloace de protecție speciale (precum „plicurile sigilate").

c) În procesul de structurare al înregistrărilor DES, trebuie acordată atenție şi **solicitărilor de date speciale** repetate. Un exemplu: Conform legislației naționale, companiile private de asigurări pot avea dreptul de a primi unele date (limitate) privind dosarele medicale, când acest lucru este necesar în contextul îndeplinirii obligațiilor contractuale față de pacienții asigurați. Autorizarea accesului pentru companiile private de asigurări la DES al unui pacient pare inacceptabilă. Din acest motiv, o soluție poate fi înființarea unui „pachet informațional" care, în situațiile necesare, satisface interesele legitime ale asiguratorului şi, dacă pacientul este de acord, poate fi transmis (electronic) companiei private de asigurări.

7. Transferul internațional al dosarelor medicale

Disponibilitatea în format electronic a datelor medicale din sistemele DES poate ameliora considerabil capacitățile de diagnostic şi tratament utilizând cunoştințele aflate exclusiv în instituții medicale externe. Consultarea suplimentară a experților străini în scopuri de diagnosticare nu implică, de obicei, dezvăluirea identității pacientului. Prin urmare, dacă este posibil, astfel de date trebuie transferate în afara Uniunii Europene/Spațiului Economic European exclusiv **sub formă anonimă sau de pseudonim**. Dacă nu există un consimțământ explicit al persoanei vizate privind transferul datelor cu caracter personal[29], aceasta va evita şi necesitatea obținerii acordului pentru acest transfer de date, deoarece persoana vizată nu poate fi identificat de către destinatar.

Având în vedere riscul important la care sunt supuse datele cu caracter personal într-un sistem DES fără protecție adecvată, Grupul de lucru pentru articolul 29 doreşte să sublinieze că orice prelucrare – în special stocarea – de date DES trebuie să aibă loc în interiorul jurisdicțiilor care aplică Directiva Uniunii Europene privind Protecția Datelor sau un alt cadru adecvat pentru protecția datelor.

O problemă specifică este constituită de fluxurile de date transfrontaliere în cursul studiilor clinice: grupul de studiu aflat în contact direct cu pacienții poate solicita câteodată acces la datele DES în forma lor originală şi personalizată. Pentru toate transferurile de date rezultate în urma studiilor clinice către sponsori sau alte instituții implicate conform legii, pseudonimele securizate trebuie totuşi să constituie o condiție prealabilă minimă, în special dacă astfel de sponsori au sediul în țări fără o protecție adecvată a datelor.

---

[28] Avantajul unui asemenea modul despre medicație în cadrul DES poate fi dublu, deoarece va acorda medicului care administrează tratamentul oportunitatea de a cunoaşte întreaga medicație prescrisă pacientului.

[29] În situațiile în care un pacient se află în incapacitatea fizică de a-şi manifesta opțiunea (de ex. deoarece se află în comă) datele sale medicale, conform articolului 26 alineatul (1) litera (e) al directivei, pot fi transferate totuşi în țări fără mijloace de protecție adecvate a datelor dacă interesele sale o reclamă.

O atenție specială trebuie acordată întotdeauna în acest context aspectelor de protecție a datelor, pentru a fi evitat riscul dezvăluirii neautorizate în medii nesigure din punct de vedere al protecției datelor.

8. Securitatea datelor

Acceptabilitatea unui sistem de prelucrare a datelor cu un potențial de risc excepțional depinde de un nivel corespunzător înalt de securitate a datelor pentru funcționarea completă a sistemului. **Accesul persoanelor neautorizate trebuie să fie practic imposibil şi prevenit**, dacă se doreşte ca sistemul să fie acceptabil din punctul de vedere al protecției datelor. Cu toate acestea, disponibilitatea sistemului pentru cadrele autorizate trebuie să fie practic nelimitat pentru cazurile când informația este absolut necesară, pentru ca sistemul să ofere avantajele promise în tratamentul medical al pacienților.

Cadrul legal pentru înființarea unui sistem DES va trebui să prevadă necesitatea punerii în aplicare a unei serii de măsuri de natură tehnică şi organizatorică pentru prevenirea distrugerii sau modificărilor, prelucrării şi accesului neautorizat la datele din sistemul DES. Integritatea sistemului trebuie să fie garantată prin exploatarea cunoştințelor şi instrumentelor reprezentând cele mai recente evoluții din domeniile informaticii şi a tehnologiei informației.

Tehnologiile de creştere a confidențialității (PET)[30] trebuie aplicate la maximă capacitate pentru a promova protecția datelor cu caracter personal. Encriptarea nu trebuie utilizată exclusiv pentru transferuri, ci şi pentru stocarea de date în sistemele DES. Toate măsurile de securitate trebuie să fie uşor de utilizat pentru a beneficia de o sferă de aplicare mai largă. Costurile necesare trebuie să fie considerate o investiție în compatibilitatea sistemelor DES cu drepturile fundamentale, aceasta constituind una dintre cele mai importante condiții pentru succesul sistemelor DES.

Indiferent de faptul că multe dintre mijloacele de protecție menționate mai sus conțin deja elemente de securitate a datelor, cadrul legal privitor la măsurile de securitate trebuie să prevadă necesitatea de

- a dezvolta un sistem durabil şi eficient pentru identificarea şi prelucrarea electronică, precum şi de a actualiza constant registrele de identificare pentru verificarea autorizării persoanelor care posedă sau solicită acces la sistemul DES;
- urmărire a activității şi documentare a tuturor etapelor prelucrării care au avut loc în sistem, în special a solicitărilor de citire şi introducere de date, împreună cu verificările interne periodice şi examinare a autorizărilor corecte;
- mecanisme eficiente de rezervă şi recuperare necesare pentru securizarea conținutului sistemului;
- prevenirea accesului neautorizat sau distrugerea datelor DES în momentul transferului sau stocării de rezervă, de ex. prin utilizarea algoritmilor de criptare;
- instrucțiuni clare şi documentate pentru toți utilizatorii autorizați privind utilizarea corectă a sistemelor DES şi evitarea riscurilor şi breşelor de securitate;
- o distincție clară între funcțiile şi competențele categoriilor de persoane însărcinate cu funcționarea sistemului sau cel puțin implicate în funcționarea acestuia, în vederea stabilirii responsabilităților pentru neajunsuri;
- audit intern şi extern periodic privind protecția datelor.

[30] În privința PET-urilor, vezi punctul 4.3 din "Primul raport privind aplicarea Directivei privind Protecția Datelor (95/46/CE)", COM (2003) 265 final.

9. Transparența

Pare evident că un DES poate contribui în mod considerabil la tratamentele medicale, dar este supus în principiu şi utilizării abuzive în urma accesului neautorizat. Opinia publică şi indivizii vor solicita prin urmare o extra **transparență privind conținutul şi funcționarea unui sistem DES** pentru a fi menținută încrederea în sistem. **Notificarea** către autoritățile de control pentru protecția datelor, împreună cu **informația specială, larg disponibilă şi uşor inteligibilă** trebuie să fie asigurată de către managerul (managerii) sistemului. Utilizarea Internetului ca mijloc ideal de transmitere a datelor poate contribui la crearea transparenței necesare pentru sistemele DES înființate la nivel național.

Punctele de acces cu acces gratuit, uşor de utilizat dar sigure, pentru uzul subiecților datelor în scopul verificării conținutului şi confidențialității propriului dosar DES poate constitui, de asemenea, o contribuție utilă la transparența şi încrederea în sistem.

10. Răspunderea

Orice sistem DES trebuie să garanteze şi că **posibilele încălcări ale confidențialității** provocate de modul de stocare şi furnizare a de date medicale într-un sistem DES sunt corespunzător **compensate de răspunderea pentru daunele** cauzate de ex. prin utilizarea incorectă sau neautorizată a datelor DES.

Într-o analiză a posibilelor probleme ale sistemelor DES din punctul de vedere al protecției datelor, problemele responsabilității pentru utilizarea incorectă a unui sistem DES pot fi doar amintite. În opinia Grupului de lucru, orice stat membru care doreşte să introducă un sistem DES trebuie să întocmească în avans studii experte de drept civil şi medical şi evaluări de impact pentru a clarifica noile aspecte ale răspunderii care pot apare în acest context, de ex. privind corectitudinea şi exhaustivitatea datelor introduse în DES, definirea măsurii în care un cadru medical ce tratează un pacient poate avea acces la DES, sau despre consecințele prevăzute de legea răspunderii dacă accesul nu este disponibil din motive tehnice etc.

11. Mecanismele de control pentru prelucrarea datelor în DES

Având în vedere **situația specială de risc** creată de înființarea sistemelor DES, **mecanisme eficiente de control** pentru evaluarea mijloacelor de protecție sunt necesare. Complexitatea datelor conținute într-un DES, împreună cu multitudinea de posibili utilizatori poate necesita noi proceduri privind drepturile de acces ale persoanelor vizate:

a) O **procedură specială de arbitraj** trebuie pusă la punct **pentru disputele** privind utilizarea corectă a datelor în sistemele DES; persoanele vizate trebuie să aibă capacitatea de a utiliza o astfel de procedură cu uşurință şi în mod gratuit. Având în vedere că, în mod obişnuit, expertiza medicală specializată va fi necesară pentru evaluarea reclamațiilor privind datele false sau prelucrate fără justificare într-un sistem DES, autoritățile de control pentru protecția datelor se pot dovedi ca nefiind cele mai recomandate pentru rezolvarea unor astfel de reclamații, cel puțin nu în primă fază. „Avocații" publici ai „pacienților", acolo unde există deja, pot primi această sarcină.

b) Un sistem DES trebuie să g că persoana vizată poate să îşi exercite drepturile de acces fără dificultăți. În principiu, managerul de date este cel obligat să acorde dreptul de acces. **Sistemele DES sunt** totuşi **sisteme de baze de date** cu multipli manageri de date. În astfel de sisteme cu un număr semnificativ de manageri de date implicați, **o singură instituție trebuie să fie responsabilă în fața persoanelor vizate pentru controlul solicitărilor de acces**. În vederea complexității previzibile a unui DES complet dezvoltat şi a necesității câştigării încrederii pacienților în sistem, pare fundamental ca pacienții a căror date sunt prelucrate într-un sistem DES să aibă acces la un lucrător pe care îl pot consulta în privința posibilelor

neajunsuri ale sistemului DES. Reglementările speciale în acest scop vor trebui incluse în toate normele de funcționare a sistemelor DES.

c) Pentru a contribui la creşterea încrederii, poate fi introdusă o **procedură specială pentru informarea persoanei vizate în privința momentului şi persoanei care a accesat datele din DES său**. Furnizarea unei liste subiecților datelor conținând persoanele sau instituțiile care le-au accesat datele va întări încrederea pacienților în privința securității propriilor date din sistemul DES.

d) Auditul intern şi extern periodic privind protecția datelor protocoalelor de acces trebuie să aibă loc. Menționatul raport anual al accesărilor trimis subiecților datelor poate constitui un mijloc adițional eficient pentru verificarea legalității accesului la datele DES. Consilierii de protecție a datelor din spitalele care participă la sistemele DES vor contribui cu siguranță la utilizarea corectă a datelor din aceste sisteme.

IV. CONCLUZII

Toți indivizii şi pacienții au dreptul la confidențialitate şi pot pretinde în mod rezonabil ca protecția şi confidențialitatea propriilor date cu caracter personal să fie menținute riguros de către cadrele medicale. Această speranță este îndreptățită şi în privința sistemelor dosarelor electronice de sănătate (DES).

Grupul de lucru pentru articolul 29 a redactat acest Document de lucru pentru a oferi asistență în interpretarea cadrului legal în vigoare privind protecția datelor pentru sistemele de dosare electronice (DES) şi pentru instituirea unor principii generale. Documentul de lucru mai intenționează să stabilească precondițiile de protecție a datelor pentru înființarea unui sistem DES național, precum şi mijloacele de protecție aplicabile, şi să contribuie la aplicarea uniformă a măsurilor naționale care decurg din Directiva 95/46/CE.

Grupul de lucru pentru articolul 29 subliniază că înființarea şi funcționarea sistemelor DES trebuie să fie pe deplin conformă principiilor de protecție a datelor cu caracter personal, precum au fost stabilite în Directiva 95/46/CE. Grupul consideră că respectarea acestor condiții slujeşte interesele tuturor persoanelor şi instituțiilor implicate în asigurarea funcționării corecte a unor astfel de sisteme. În plus, Grupul de lucru pentru articolul 29 accentuează necesitatea înființării şi funcționării sistemelor DES într-un cadru legal sănătos de mijloace de protecție dedicate protecției datelor cu caracter personal, indiferent de bazele legale ale unor asemenea sisteme.

Grupul de lucru pentru articolul 29 invită medicii, tot personalul medical, persoanele şi instituțiile implicate în furnizarea de servicii medicale, precum şi publicul larg, să îşi prezinte opinia asupra acestui Document de lucru.[31]

Având în vedere dezvoltarea continuă din acest domeniu, pot fi necesare activități ulterioare, observații suplimentare şi noi contribuții ale Grupului de lucru pentru articolul 29.

---

[31] Observațiile la acest Document de lucru vor fi trimise la: Secretariat of the Article 29 Working Party
European Commission, Directorate-General Justice, Freedom and Security
Unit C.5 – Protection of personal data
Office: LX 46 1/43
B - 1049 Brussels
E-mail: Amanda.JOYCE-VENNARD@ec.europa.eu ; Fax: +32-2-299 80 94
Toate observațiile provenite din sectoarele public şi privat vor fi publicate pe adresa de Internet a Grupului de lucru pentru articolul 29, cu excepția cazurilor când corespondenții îşi manifestă dorința ca datele lor să nu fie date publicității.

Adoptat la Bruxelles, la 15 februarie 2007

Pentru Grupul de lucru
Preşedinte
Peter SCHAAR