privacyONE
in alliance with BIRIŞ·GORAN Legal + Tax

GDPR in sistemul de sanatate

Aspecte principale

12 decembrie 2018

Andreea Lisievici, CIPP/E, avocat

Legea 46/2003 privind drepturile pacientului

Art. 21

Toate informațiile privind starea pacientului, rezultatele investigațiilor, diagnosticul, prognosticul, tratamentul, datele personale **sunt confidențiale chiar şi după decesul acestuia**.

“Se interzice prelucrarea de date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de **date privind sănătatea** sau de date privind viața sexuală sau orientarea sexuală ale unei persoane fizice.”

Art. 9(1) GDPR

privacyONE

CJEU, C-101/01 *Bodil Linqvist*, 2003, par 50

50. In the light of the purpose of the directive, the expression 'data concerning health' used in Article 8(1) thereof must be given a **wide interpretation** so as to include information concerning all aspects, **both physical and mental**, of the health of an individual.

Opinia 4/2007 privind conceptul de date cu caracter personal (WP136)

Ce inseamna a prelucra date personale?

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

Avem o restrictie. Ce facem cu ea?

- **Legea 46/2003 privind drepturile pacientului**
  - Informațiile cu caracter confidențial pot fi furnizate numai în cazul în care pacientul îşi dă **consimțământul explicit sau dacă legea o cere în mod expres**. (art. 22)
  - În cazul în care informațiile sunt **necesare altor furnizori de servicii medicale acreditați, implicați în tratamentul pacientului, acordarea consimțământului nu mai este obligatorie**. (art. 23)
- **GDPR**
  - Conditie generala: existenta unui **temei** al prelucrarii conform art. 6
  - Conditie speciala: existenta unuia din **cazurile de exceptie** de la art. 9(2).

Legea 46/2003 privind drepturile pacientului

- Priveste exclusiv DIVULGAREA datelor pacientului, iar nu prelucrarea datelor chiar de catre medic, in activitatea sa

GDPR

- Priveste INTREAGA PRELUCRARE a datelor pacientilor: atat practica proprie a medicului, cat si orice alt tip de prelucrare
  - folosirea serviciilor terte, studii clinice, arhivare, pierdere, etc

Cele doua legi privesc ipoteze diferite

Art. 6 GDPR - temeiurile prelucrarii in general

persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice

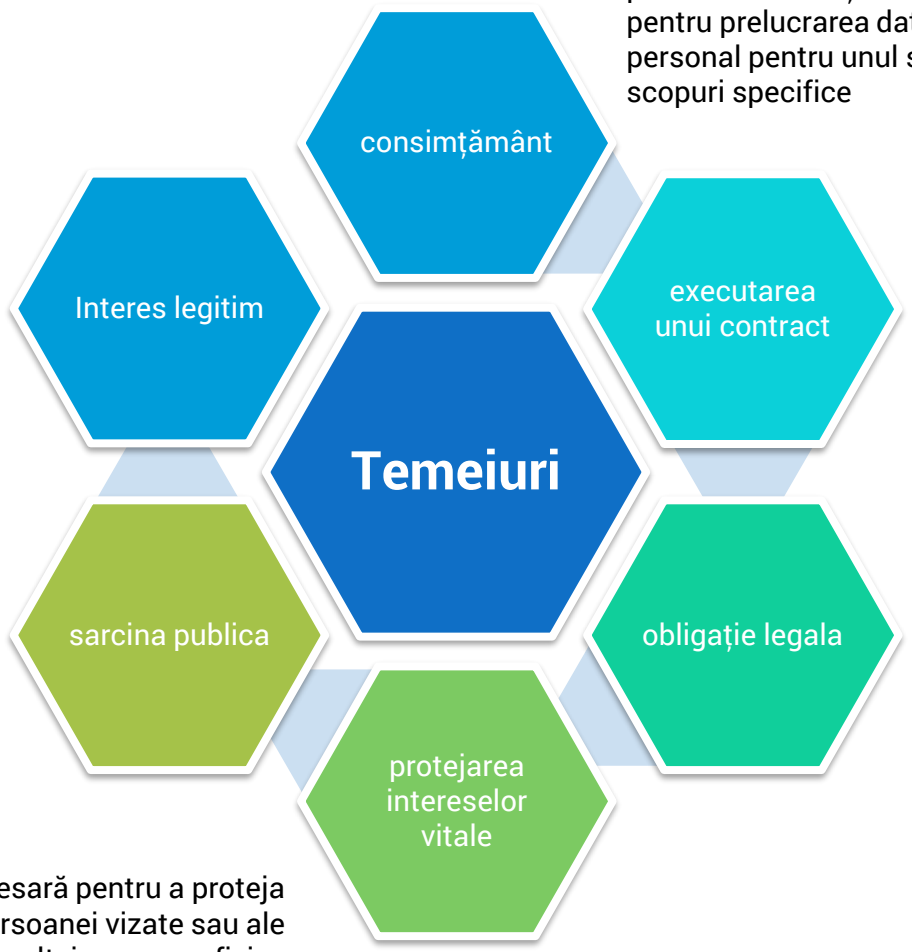
prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de un terț

prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract

prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul

prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului

prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice



Art. 9 GDPR – conditii speciale pentru prelucrarea datelor sensibile

1. consimtamant
2. drepturi si obligatii în domeniul ocupării forței de muncă și al securității sociale și protecției sociale, dacă acest lucru este autorizat de lege sau de un acord colectiv de muncă
3. **protejarea intereselor vitale ale persoanei vizate** sau ale unei alte persoane fizice
4. Activitatea unei fundații, asociații sau orice alt organism fără scop lucrativ și cu specific politic, filozofic, religios sau sindical
5. datele sunt făcute publice în mod manifest de către persoana vizată
6. constatarea, exercitarea sau apărarea unui drept în instanță
7. motive de interes public major
8. **medicina preventivă sau a muncii, diagnostic** (cu conditii)
9. **motive de interes public în domeniul sănătății publice**
10. arhivare în interes public, cercetare științifică sau istorică ori scopuri statistice

CE TEMEI APLICAM PENTRU PRELUCRAREA DATELOR DE SANATATE?

Este necesar consimtamantul?


Din cauza de GDPR nu mai putem chema pacientii dupa nume. Domnul cu sifilis sa intre!

Temeiul prelucrarii de date

Sector public

- Medicina de urgenta:
  - Art 6.1.e (îndeplinirea unei sarcini care servește unui interes public) si 6.1.d (protejarea intereselor vitale ale persoanei vizate) +
  - Art. 9.2.c (protejarea intereselor vitale ale persoanei vizate)
- Celelalte situații:
  - Art 6.1.e (îndeplinirea unei sarcini care servește unui interes public) +
  - Art. 9.2.h (medicina preventivă sau a muncii, diagnostic)

Temeiul prelucrarii de date

Sector privat

- Medicina de urgenta:
  - art 6.1.d (protejarea intereselor vitale ale persoanei vizate) + Art. 9.2.c (protejarea intereselor vitale ale persoanei vizate)
- Alte situatii, daca persoana nu este abonata prin angajator:
  - art. 6.1.c (executarea unui contract la care persoana vizată este parte) + art 9.2.h (medicina preventivă sau a muncii, diagnostic)
- Alte situatii, daca persoana este abonata prin angajator:
  - art. 6.1.f (interes legitim urmărit chiar de persoana vizata) + art 9.2.h (medicina preventivă sau a muncii, diagnostic)

dacă prelucrarea datelor de sănătate depăşeşte scopul acordării serviciului medical sau al protejării interesului vital al pacientului, este necesar consimțământul.

De ex: pentru marketing direct, pentru folosirea unui testimonial, pentru promovarea imaginii unității medicale, pentru filmarea unei proceduri.

Nu confundati acordul pentru actul medical cu acordul pentru prelucrarea datelor

Acordul pacientului pentru actul medical este (cu cateva exceptii) intotdeauna necesar, potrivit legii

Nu are legatura cu prelucrarea de date, prelucrarea are loc si daca actul medical nu are loc (invers nu)

Daca decideti sa cereti consimtamant pentru prelucrarea datelor, este esential sa il separati de acordul pentru actul medical

OBLIGATIILE MEDICILOR IN PRELUCRAREA DATELOR PERSONALE ALE PACIENTILOR

1. Informati pacientii
2. Limitați datele colectate la cele strict necesare și folositi-le doar conform scopurilor definite si incluse in Informare
3. Stabiliti perioade de stocare a datelor in functie de scop si stergeti datele care depasesc durata
4. Aplicati masuri adecvate de securitate
5. Verificati furnizorii cu acces la datele pacientilor
6. Pastrati un registru al activitatilor de prelucrare

Informarea pacientilor cu privire la prelucrarea datelor

Obligativitatea informarii

Indiferent de temeiul ales pentru prelucrare, informarea este obligatorie atunci cand datele sunt obtinute direct de la pacient

Daca datele sunt obtinute din alta parte, informarea este obligatorie, mai putin daca:

1. Informarea se dovedește a fi imposibilă sau ar implica eforturi disproporționate, ori este susceptibil să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării
   - *Este totusi necesara o informare publica*
2. obținerea sau divulgarea datelor este obligatie legala
3. datele cu caracter personal trebuie să rămână confidențiale în temeiul unei obligații statutare de secret profesional reglementate de lege

Ce trebuie sa contina informarea – varianta lunga

- ✓ numele si datele de contact ale operatorului; datele de contact ale DPO, daca exista;
- ✓ scopurile prelucrarii si temeiul legal, incluzand precizarea interesului legitim daca este folosit;
- ✓ categoriile de destinatari
- ✓ daca se transfera date in tari terte, garantiile de adecvare folosite
- ✓ durata de pastrare a datelor
- ✓ drepturile persoanei vizate
- ✓ posibilitatea retragerii consimtamantului
- ✓ dreptul de a depune o plângere la ANSPDCP
- ✓ dacă furnizarea de date cu caracter personal reprezintă o obligație legală sau contractuală sau o obligație necesară pentru încheierea unui contract, precum și dacă persoana vizată este obligată să furnizeze aceste date cu caracter personal și care sunt eventualele consecințe ale nerespectării acestei obligații
- ✓ Daca exista un proces decizional automatizat, precum și informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări

Ce trebuie sa contina informarea – varianta scurta

- Cine colecteaza date?
- Ce date?
- De ce? (cu ce scop si in ce baza legala)
- Cum vor fi folosite datele si de catre cine? Vor fi implicati terti?
- Datele vor fi transferate altor entitati? Daca da, de ce?
- Ce urmari va avea prelucrarea? Dar lipsa ei?
- Ce optiuni au persoanele si ce pot face daca au intrebari sau nemultumiri?
- Dacă este cazul, utilizarea ulterioară a datelor în alt scop decât cel pentru care au fost colectate datele (de ex.: dacă un medic dorește să utilizeze datele în scopuri de cercetare)

Cand si cum se face informarea

- Informarea trebuie facuta inainte de colectarea datelor – la momentul primului contact
- Nu este necesara semnatura pacientului
- Gasiti metode eficiente care sa asigure informarea nu doar initial, ci sa poata fi regasita la orice moment apoi, in loc sa cautati sa va acoperiti de hartii
- Ganditi-va ca pacientii nu pastreaza hartii, este mai eficienta comunicarea pe alt canal

De exemplu

- Email trimis la inscrierea in sistem – mai ales la inscrierea de catre terti, cum sunt angajatorii
- Varianta scurta a informarii, cu design placut si atragator, la receptie si/sau pe ecranele din sala de asteptare
- Postarea informarii pe site si includerea unui link catre ea in toate comunicarile electronice cu pacientul (email / sms)
- Includerea unui privacy dashboard in platformele cu cont de utilizator, unde pacientul sa poata sa isi acceseze optiunile (de ex. acord pentru marketing) si sa isi exercite drepturile

Informarea adresata pacienților si pusa pe website nu trebuie să se confunde cu o eventuală informare despre prelucrarea datelor prin intermediul website-lui.

Minimizarea datelor si limitarea la scop

De ce se prelucreaza date in activitatea medicala?

- Scopul principal al activitatii unui medic este reprezentat de prevenția medicala, stabilirea diagnosticului și acordarea îngrijirii medicale
- Datele stranse in acest scop beneficiaza de o larga masura de apreciere, cuprinzand cel putin:
  - gestionarea programărilor;
  - gestionarea fiselor medicale;
  - emiterea rețetelor;
  - decontarea în Sistemul Informatic Unic Integrat;
  - comunicarea profesionala in cadrul formei de exercitare si inafara ei;
  - comunicarea cu pacientul, inclusiv transmiterea la distanta a rezultatelor.

Nu colectati mai multe date decat este necesar in fiecare caz

- **Date necesare ca regula**:
  - datele de identificare: numele, prenumele, data nașterii, adresa, numărul de telefon;
  - numarul cardului de sănătate;
  - angajator (pentru abonamente business);
  - date de sanatate: istoricul medical, istoricul tratamentelor, diagnosticele medicale, tratamentele prescrise, natura actelor efectuate, rezultatele examenelor de biologie medicală și orice element de natură să caracterizeze starea de sănătate a pacientului și considerat pertinent de către medic
- **Date necesare doar uneori** – se prelucreaza numai unde sunt necesare:
  - situația familiala: starea civila, numarul de copii
  - viata profesionala: profesia, condițiile de muncă
  - obiceiurile de viata, alimentare
  - Orientarea sexuala (doar daca are legatura cu staful medical cerut)
- **Date care de regula nu sunt necesare**:
  - Religia, opinii politice
  - originea etnică

Prelucrarea CNP

- CNP-ul este obligatoriu de folosit in sistemele si tipizatele puse la dispozitie de stat, dar in rest nu
- Minimizati pe cat posibil prelucrarea CNP, este data personala cu regim special
  - Nu puneti CNPul pe rezultatele investigatiilor
  - Nu folositi CNPul ca identificator in sistemul vostru, de ex. la call center sau in sistemul de conturi online
- Pe langa excesivitatea unei asemenea prelucrari, este un tip de prelucrare efectuata in interesul vostru legitim, ceea ce atrage necesitatea sa numiti un responsabil cu prelucrarea datelor (art. 4 din Legea nr. 190/2018)

- Orice altă utilizare a datelor pacientilor trebuie să fie realizată numai cu acordul acestora
  - de ex. profilare si trimitere de recomandari personalizate (marketing direct)

- Utilizarea personală sau comercială a datelor pacientilor este interzisă
  - daca pacientul nu se asteapta, in mod rezonabil, ca o anumita prelucrare sa aiba loc, atunci ar trebui sa nu aiba loc decat cu informare si consimtamant prealabil

- Restrictiile se aplica si furnizorilor care au acces la date (de ex. furnizorii de software)
  - ei prelucreaza datele ca imputerniciti, in numele unitatii medicale, care este principalul responsabil pentru legalitatea intregii prelucrari

Stabiliti perioade de stocare a datelor

Perioada de pastrare a datelor medicale

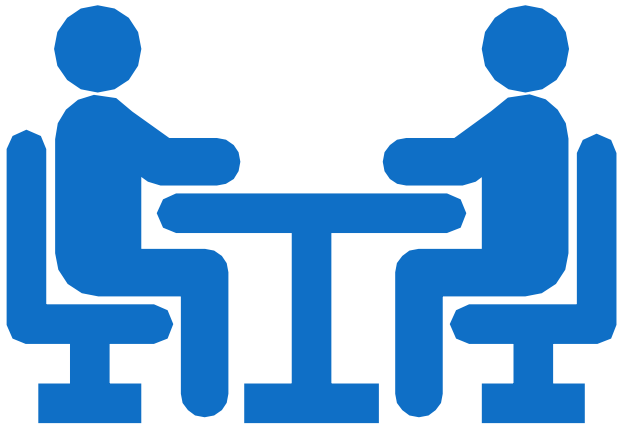
- In Romania sunt foarte rare cazurile cand legea cere pastrarea datelor pentru un termen minim

- Ordinul National al Medicilor din Franta recomanda:

  - 20 de ani de la data ultimei consultări a pacientului;
  - dacă pacientul este minor și acest termen de 20 de ani expiră înainte ca acesta să împlinească 28 de ani, păstrarea datelor sale trebuie să fie prelungită până la această dată;
  - dacă pacientul decedează în termen de sub 10 ani de la ultima sa consultație, informațiile referitoare la el trebuie să fie păstrate timp de 10 ani începând de la data decesului;
  - în cazul unei actiuni pentru tragerea la răspundere a medicului, termenul se suspenda si datele nu se distrug indiferent cat timp trece pana la finalizare, urmand sa continue dupa aceea.

Spre deosebire de dosarele pacientilor, care justifica o durata de păstrare destul de indelungata, datele legate de programari pot fi sterse mult mai repede, fiind greu de crezut ca se justifica o perioada mai mare de un an

Securitatea datelor



Limitati cine are acces la datele medicale

- Personalul administrativ nu trebuie sa aiba acces global la dosarele medicale, ci doar la acele date care sunt necesare functiilor lor
  - Acorduri de confidentialitate necesare pentru personal
- Cea mai delicata situatie – furnizorii care au acces la datele pacientilor (software, mentenanta IT, arhivare)
  - Toti acestia sunt imputerniciti, supusi unui regim distinct potrivit GDPR

Securizarea sistemului informatic

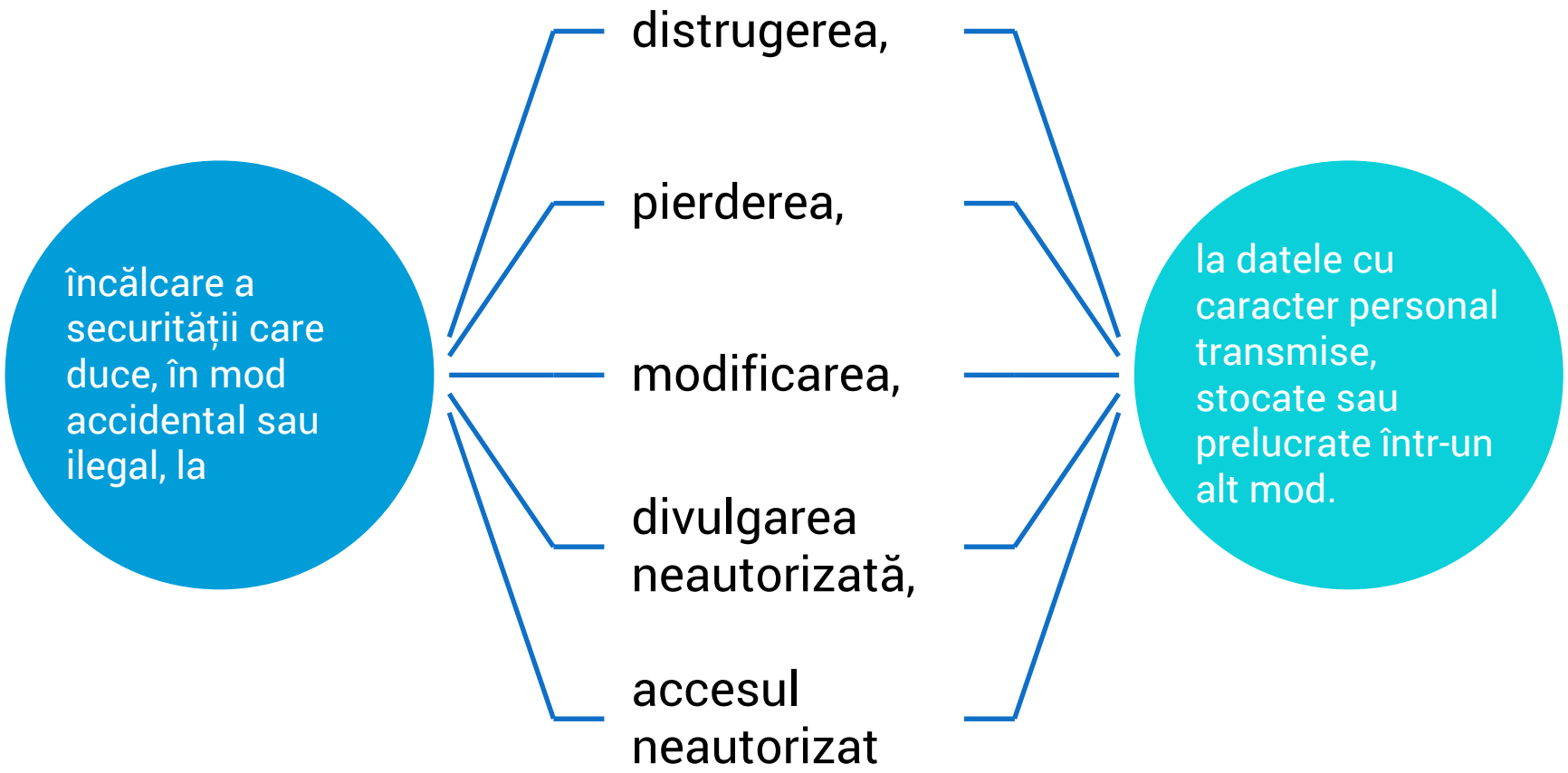
Trebuie sa va auditati nevoile si sa implementati masuri adecvate, cum ar fi:

- parole complexe, modificate cu regularitate;
- blocarea sesiunii automat dupa un interval predefinit de inactivitate;
- antivirus actualizat, firewall, aplicarea sistematică a patch-urilor și update-urilor de securitate;
- back-up cu redundanta geografica, efectuat la intervale scurte (de ex. o data pe saptamana);
- criptarea datelor;
- blocarea accesului in retea a terminalelor personale neautorizate;
- folosirea unui mijloc de autentificare puternica (2FA, amprenta).

Daca intervine o incalcare a securitatii datelor

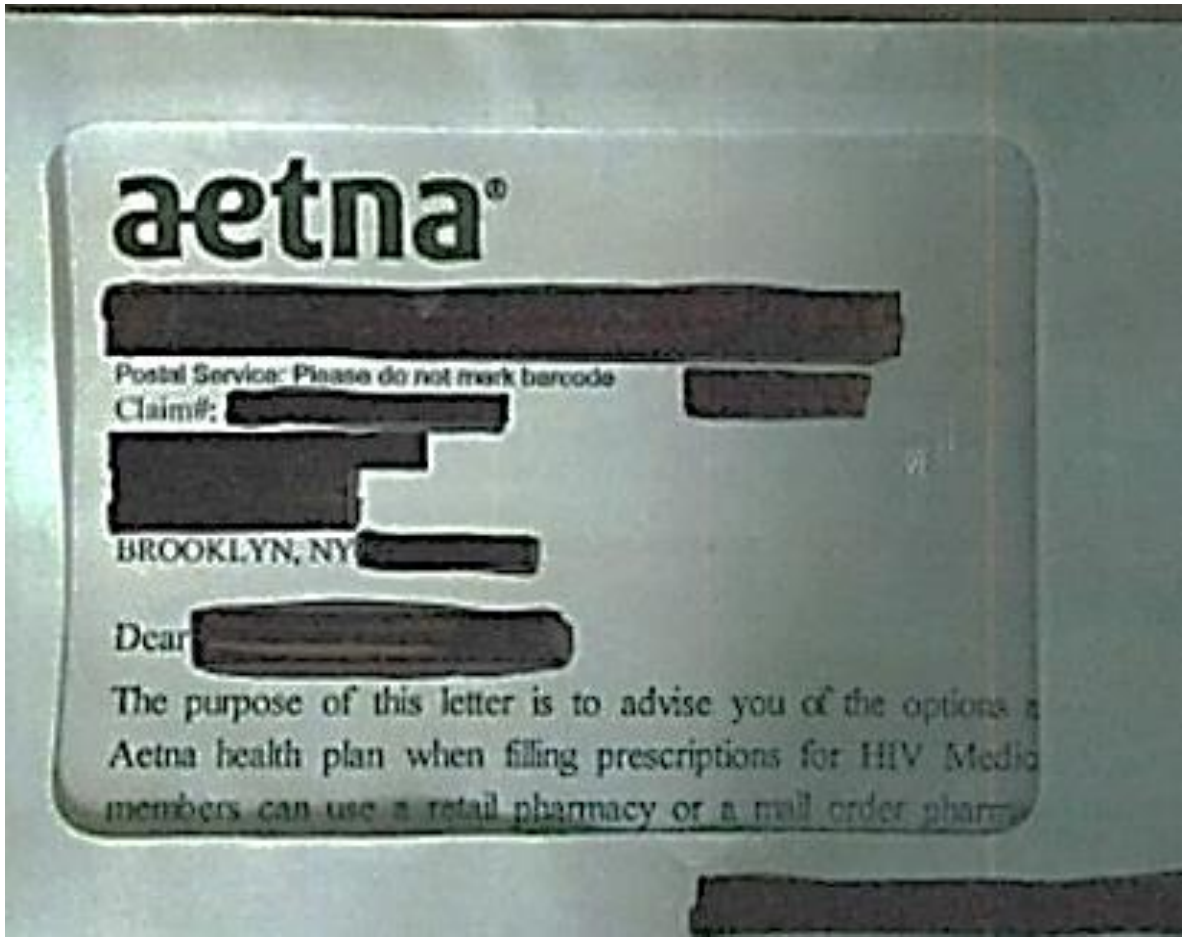
1. analizati amploarea problemei pentru a identifica demersurile pe care trebuie să le faceti si sa evitati repetarea acestui incident:
   - cine a avut acces la date?
   - care este originea problemei?
   - datele au fost transmise unui tert?
   - sunt implicate datele de sanatate?
   - ce masuri ar fi putut impiedica evenimentul sau ce masuri ar putea atenua consecintele?
2. daca exista un risc pentru drepturile si libertatile persoanelor, notificati ANSPDCP in 72 de ore de cand ati luat cunostinta – formular pe site
3. Daca riscul este ridicat, trebuie să informati si persoanele afectate, cu exceptia cazului în care datele erau criptate (a.i. citirea este imposibila), sau daca masurile luate ulterior garanteaza ca riscul ridicat nu se mai poate materializa
   - comunicare individuala

Incalcare a securitatii datelor



- *Analizele medicale RMN au fost trimise din greşeală altui pacient prin e-mail. ANSPDCP a considerat că nu s-au aplicat măsuri tehnice şi organizatorice adecvate pentru protejarea datelor personale împotriva accesului neautorizat.*
  - Raportul anual ANSPDCP din 2017 (p. 74)

- *Corespondența despre analize şi alte proceduri era trimisă constant către adresa de e-mail greşită (diferența dintre cele două adrese de e-mail fiind un punct intre nume – de exemplu, ionpopescu şi ion.popescu).*
  - Raportul anual ANSPDCP din 2017 (p. 104)



https://www.hipaajournal.com/aetna-seeks-least-20-million-damages-firm-responsible-hiv-status-data-breach/

Aetna Seeks At Least $20 Million in Damages from Firm Responsible for HIV Status Data Breach

In the lawsuit, Aetna claims the firm's errors and omissions amounted to gross negligence and that KCC should have been aware that HIV medication information was detailed under the names and addresses of its plan members. Aetna claims no checks were performed to determine how much information was visible through the windows of the envelopes. Aetna also claims KCC did not communicate to Aetna that envelopes with clear plastic windows were being used for the mailing, and that Aetna's lawyers were not consulted to give their approval of the mailing.

Cerinte privind imputernicitii

Cerinte privind imputernicitii

Operatorul trebuie sa foloseasca numai imputerniciti care oferă garanții suficiente astfel încât prelucrarea să respecte GDPR

- Verificarea imputernicitilor

Prelucrarea de catre imputernicit trebuie reglementata de un contract care sa contina anumite elemente minime

- Acorduri de prelucrare de date

Verificarea imputernicitilor

- In alte tari exista certificari speciale pentru furnizorii care asigura stocarea datelor de sanatate
- Chiar daca la noi in tara nu exista ceva similar, tot trebuie sa documentati verificarea pe care o faceti
  - Nu ajunge sa cereti o declaratie de la furnizor ca este “GDPR compliant”
  - Uitati-va dupa ISO 9004, ISO 27001 si altele asemenea

Cerinte minime pentru contractele cu imputernicitii

- nu prelucrează datele cu caracter personal decât conform instrucțiunilor operatorului;
- asigura angajamentele de confidențialitate de către personal;
- ia toate măsurile de securitate impuse;
- nu recrutează niciun subimputernicit fără acordul prealabil scris al operatorului;
- asista operatorul atunci când este necesar pentru indeplinirea obligatiilor sale;
- sterge sau înapoiază datele cu caracter personal după finalizarea actvitatilor;
- colaborează în cadrul auditurilor.

De ce este importanta relatia cu imputernicitii

Operator

Operatorul este răspunzător pentru prejudiciul cauzat de operațiunile sale de prelucrare care încalcă GDPR. Operatiunile imputernicitului sunt tot ale operatorului!

Ca principiu, operatorul este raspunzator pentru activitatea desfasurata in numele sau de imputernicit

Imputernicit

Împuternicitul este răspunzător pentru prejudiciul cauzat de prelucrare numai în cazul în care

1. nu a respectat obligațiile din GDPR care revin în mod specific persoanelor împuternicite sau
2. a acționat în afara sau în contradicție cu instrucțiunile legale ale operatorului.

Cateva chestiuni despre relatia cu clientii corporate

Calitatea prestatorului de servicii medicale în raport cu clienții corporate

Furnizorul de servicii medicale nu este niciodata imputernicit, nici in serviciile de medicina muncii nici in cele la cerere, intrucat el nu isi organizeaza activitatea dupa instructiunile clientului, ci conform regulilor stabilite de lege si de etica medicala

Informarea pacientilor

- In calitate de operator de date, aveti intotdeauna obligatia de a informa pacientii
- Nu este eficient sa cereti clientilor corporate sa informeze ei angajații pentru voi, incercati tot timpul sa faceti voi direct
  - Riscul lipsei informarii sau informarii incomplete il suportati doar voi
  - Nu cedati controlul asupra acestei chestiuni importante
  - Nu insistati pe semnaturi de la pacienti, cu atat mai putin colectate de alta entitate
- Aveti 30 de zile de la momentul cand primiti datele (sau la prima comunicare cu persoana) sa faceti informarea
- Configurati sistemul ca la introducerea unui abonat sa i se trimita automat informarea pe email

REGISTRUL ACTIVITATILOR DE PRELUCRARE

De ce acest registru?

notificarea la ANSPDCP nu mai este aplicabila, însă operatorii si imputernicitii trebuie sa mențină o evidență a activităților de prelucrare desfășurate sub responsabilitatea lor

Ce conține registrul tinut de operator

a) numele și datele de contact ale operatorului și ale DPO;

b) scopurile prelucrării;

c) categoriile de persoane vizate și categoriile de date cu caracter personal;

d) categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele;

e) dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională, documentația care dovedește existența unor garanții adecvate;

f) acolo unde este posibil, termenele-limită preconizate pentru ștergerea diferitelor categorii de date;

g) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate (MTOS) menționate la art. 32(1).

Cum se tine registrul

- Limba – nu exista cerinta speciala dar trebuie sa fie accesibil autoritatii de supraveghere
- Forma - în scris, inclusiv în format electronic
  - nu exista un format prestabilit, fiecare operator este liber sa aleaga forma care i se potriveste
- Acuratete – registrul trebuie actualizat la zi
- Fiabilitate – este indicat ca modificarile sa fie logate, si sa nu fie permise decat unor persoane limitate (privacy by design)

Resurse

- Model CNIL pentru registru: https://www.cnil.fr/sites/default/files/atoms/files/registre-reglement-publie.xlsx
- Model ICO pentru registru (si explicatii): https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/documentation/how-do-we-document-our-processing-activities/

privacyONE

ESTE NECESAR UN RESPONSABIL CU PROTECTIA DATELOR?

Este necesara numirea unui DPO daca

- prelucrați date de sănătate la scară largă
  - centru de sanatate, clinica
- prelucrati CNP in interes legitim

Daca exercitati profesia in mod individual, nu este necesara numirea unui DPO cata vreme nu prelucrati CNP in interes legitim

Thank you!

privacyONE
in alliance with BIRIŞ·GORAN Legal + Tax

Bd. Aviatorilor nr. 47, etaj 2
Bucharest, Sector 1

www.privacyone.ro

contact@privacyone.ro