



BULETIN DE PROTECȚIA DATELOR (GDPR)

Nr. 3 • Septembrie 2026

O poză, un mesaj:

datele pacienților pe WhatsApp și în fotografii

Material informativ pentru personalul instituției

Elaborat de DAF Consulting & Management SRL – responsabil cu protecția datelor (DPO) extern

De ce primiți acest material

WhatsApp-ul și camera telefonului sunt utile și omniprezente. Exact de aceea au devenit cea mai comodă — și cea mai riscantă — scurtătură pentru date medicale.

Zero

control mai are instituția asupra unei fotografii cu date de pacient odată trimisă pe WhatsApp: copii pe telefoane private, backup-uri automate în cloud, redistribuiri.



Date de sănătate = protecție maximă

Diagnostiche, foi de observație, imagini medicale sunt „categorii speciale de date” (art. 9 GDPR) — cele mai strict protejate de lege.



Telefonul personal nu e infrastructura instituției

WhatsApp-ul personal nu are contract cu instituția, nu e controlat de IT și duce datele pe servere din afara ei.



Incidente reale, frecvente

Poze cu documente medicale ajunse în grupuri greșite sau publice au produs sancțiuni și scandaluri în spitale — inclusiv în România.

Cum se întâmplă, de fapt

Patru gesturi făcute zilnic, cu cele mai bune intenții:



Poza „pentru rapiditate”

Fotografia după foaia de observație sau rezultat, trimisă colegului „ca să nu mai scriu”. Documentul medical e acum pe două telefoane personale.



Grupul de secție

Discuții despre cazuri cu nume, salon sau detalii identificabile — într-un grup unde nu toți membrii au „nevoia de a ști”.



Pacientul din fundal

Selfie-uri, poze de la evenimente sau din secție în care apar pacienți, ecrane cu date sau documente lăsate pe birou.



Rezultatele „pe WhatsApp”

Trimiterea analizelor către pacient pe numărul personal al angajatului — în afara oricărui canal oficial și verificabil al instituției.

De ce e o problemă — chiar „între colegi”

Nu intenția e problema, ci traseul datelor. Odată plecată de pe sistemele instituției, informația:



Urcă automat în cloud personal

Backup-ul telefonului copiază pozele și conversațiile în conturi private (Google/Apples) — în afara oricărui control al instituției.



Rămâne la foști angajați

Cine pleacă din instituție rămâne cu istoricul grupului — și cu toate datele de pacienți discutate vreodată acolo.



Stă pe telefoane nesecurizate

Telefon personal pierdut, fără cod de blocare, folosit și de copii — iar în galerie: documente medicale.



Membrii grupului nu sunt verificați

Numere schimbate, persoane adăugate din greșeală, grupuri „de secție” cu externi — nimeni nu garantează cine citește.



Nu există temei legal

Instituția nu are contract de prelucrare cu WhatsApp pentru date medicale, iar pacientul nu a consimțit la acest canal.



Nu se mai poate șterge cu adevărat

„Șterge pentru toți” nu atinge capturile de ecran, backup-urile și redistribuirile deja făcute. Ce a plecat, a plecat.

Fotografiile în instituție: patru reguli



Fotografierea pacienților — doar cu consimțământ și scop clar

În scop medical documentat (ex. evoluția unei plăgi), pe echipamentele și în sistemele instituției — niciodată „din reflex” pe telefonul personal.



Atenție la fundal

Înainte de orice fotografie în instituție: verificați ce se vede în spate — pacienți, monitoare cu date, foi de observație, liste de pe birouri.



Evenimente și imagini de prezentare

Fotografiile de la evenimente sau pentru site/social media trec prin purtătorul de cuvânt / conducere — nu se postează individual.



Social media: pacientul nu este conținut

Nicio imagine, poveste sau detaliu despre pacienți pe conturile personale — nici „anonimizat” aproximativ, pentru că un salon, o dată și un detaliu ajung pentru identificare.

Regula de aur

GÂNDEȘTE-TE • PROTEJEAZĂ • CANAL OFICIAL



1. GÂNDEȘTE-TE

Înainte de a fotografia sau trimite: chiar e nevoie? Cine va vedea? Ar fi în regulă dacă pacientul — sau ANSPDCP — ar citi acest mesaj?



2. PROTEJEAZĂ

Dacă există o nevoie profesională reală de a comunica un caz: fără nume, CNP, fotografii de documente sau detalii care fac persoana identificabilă.



3. CANAL OFICIAL

Datele medicale circulă prin sistemele instituției: aplicația medicală, e-mailul instituțional, folderele interne. WhatsApp-ul personal nu e canal de lucru pentru date de pacienți.

Aveți deja grupuri de WhatsApp? Reguli de igienă

Realist, grupurile există și sunt utile pentru organizare. Pot rămâne — cu limite clare:



Doar organizare, zero date de pacienți

Ture, program, anunțuri administrative — da. Nume de pacienți, cazuri identificabile, fotografii de documente — niciodată.



Curățați lista de membri periodic

Foștii angajați se scot din grup în ziua plecării. Administratorul grupului verifică lista lunar — cine nu mai e în instituție, nu mai e în grup.



Telefonul — minim securizat

Cod de blocare, actualizări la zi, fără acces al altor persoane la aplicație. Dacă telefonul se pierde, anunțați IT-ul și schimbați parolele.



Ați văzut date de pacienți în grup? Semnalați

Atrageți atenția colegului, cereți ștergerea și anunțați responsabilul intern — la nevoie și DPO. Tăcerea transformă excepția în obicei.

Pe scurt: așa NU / așa DA

Așa NU

- Nu fotografiați documente medicale cu telefonul personal
- Nu discutați cazuri identificabile în grupuri de WhatsApp
- Nu trimiteți rezultate sau date către pacienți de pe numărul personal
- Nu postați pe social media imagini sau detalii despre pacienți
- Nu păstrați foști angajați în grupurile de lucru

Așa DA

- Folosiți sistemele și canalele oficiale ale instituției pentru orice date medicale
- Păstrați grupurile de WhatsApp strict pentru organizare (ture, program)
- Verificați fundalul înainte de orice fotografie în instituție
- Securizați telefonul: cod de blocare, actualizări, fără acces terți
- Semnalați coleg(i)al orice derapaj — și către DPO dacă e cazul

A ajuns o poză sau un mesaj unde nu trebuia?

Ca la e-mailul trimis greșit (buletinul nr. 2): nu panica, ci reacția rapidă face diferența.



1. Ștergeți „pentru toți” — dar nu vă opriți aici

Ștergerea limitează expunerea, însă nu atinge capturile de ecran și backup-urile. Nu este o soluție, ci doar primul gest.



2. Anunțați imediat — intern și către DPO

O posibilă breșă se anunță întotdeauna și imediat către DPO: termenul de 72 de ore pentru evaluare și eventuala notificare ANSPDCP curge deja.



3. Notați exact ce s-a întâmplat

Ce conținea mesajul/fotografia, când a fost trimis, în ce grup, câți membri, ce persoane sunt vizate — detaliile decid evaluarea riscului.



4. Cine raportează nu este „vinovatul”

Angajatul care anunță imediat protejează pacientul și instituția. Ascunderea, nu greșeala, este adevărata problemă.



Rețineți esențialul

Ce intră pe WhatsApp nu se mai întoarce: datele pacienților rămân pe canalele instituției.

Grupurile pot rămâne pentru ture și organizare — dar fără nume de pacienți, fără cazuri identificabile și fără fotografii de documente. Iar dacă totuși s-a întâmplat: anunțați imediat, intern și către DPO.



Materialul face parte din programul lunar de informare privind protecția datelor derulat de DAF Consulting & Management SRL pentru instituțiile pe care le asistăm în calitate de responsabil cu protecția datelor (DPO) extern.

Ediția următoare (octombrie 2026): Curat pe birou, curat pe ecran — documentele lăsate la vedere.