ANEXA 8

Procedura privind managementul incidentelor de securitate

Acest document va fi de avut în vedere spre a fi aplicat mai ales dacă vă aflați într-unul din cazurile descrise în:

- Orientarea 3.12 privind **modalitatea de răspuns în caz de încălcare a securității și confidențialității datelor** pacientului sau a altei persoane vizate

Mai exact, de fiecare dată când:

- S-au pierdut date, au fost furate, au fost divulgate în mod neautorizat
- S-au distrus date de pe suporturi electronice
- Am suferit un atac cibernetic care au blocat temporar datele, etc.

Procedură privind managementul incidentelor de securitate

I. Descrierea Procedurii

I.1. Identificarea tipului de încălcare a securității datelor

Regulamentul stabileşte trei categorii de încălcări ale securităţii datelor cu caracter personal:

- **încălcarea confidenţialităţii** - în cazul în care se produce divulgarea neautorizată sau accidentală a datelor cu caracter personal sau accesul la acestea
- **încălcarea integrităţii** - în cazul în care se produce o modificare neautorizată sau accidentală a datelor cu caracter personal
- **încălcarea disponibilităţii** - în cazul în care se produce o pierdere neautorizată sau accidentală a accesului la date sau distrugerea datelor cu caracter personal

[Operatorul] face toate eforturile pentru a preveni încălcarea securităţii datelor cu caracter personal. Totuşi, este posibilă producerea unei erori sau unor evenimente care nu se află sub controlul **[Operatorul]**.

Încălcările securităţii datelor cu caracter personal se pot produce din mai multe cauze, printre care se numără și:

- pierderea sau furtul de date sau echipamente pe care sunt stocate datele (chiar dacă dispozitivul este criptat trebuie să se acorde atenţie dacă există un back-up disponibil)
- control inadecvat al accesului, care permite utilizarea neautorizată
- erori ale echipamentelor utilizate
- dezvăluirea neautorizată (de exemplu, un e-mail trimis către un destinatar incorect sau un document trimis la o adresă greşită, etc.)
- erori umane ale persoanelor care se ocupă de activitățile de prelucrare
- evenimente neprevăzute, precum incendiile sau inundaţiile
- atac cibernetic

Consecinţele unei încălcări a securităţii datelor cu caracter personal pot cauza prejudicii materiale sau morale **pentru persoanele vizate**, cum ar fi pierderea controlului asupra datelor cu caracter personal, furtul de identitate, fraudă, pierderi financiare, afectarea reputaţiei sau orice alt dezavantaj economic sau social pentru persoana vizată în cauză.

Consecinţele unei încălcări a securităţii datelor cu caracter personal **pentru [Operatorul]** includ afectarea reputaţiei şi riscurile financiare, în special în ceea ce priveşte eventualele amenzi care pot fi impuse de autoritatea de supraveghere şi despăgubirile care pot fi solicitate de persoanele vizate ale cărori drepturi au fost încălcate.

I.2. Constatarea unui incident de securitate

Oricare membru al personalului **[Operatorul]** sau altă persoană care descoperă o încălcare a securităţii datelor cu caracter personal sau crede că a avut loc o încălcare a securităţii datelor cu caracter personal, este obligată să o raporteze imediat Responsabilului cu protecția datelor sau conducerii unității medicale.

Datele de contact ale Responsabilului cu protecţia datelor din cadrul **[Operatorul]** sunt următoarele: e-mail: dpo@_____.ro

La anunţarea incidentului, persoana care îl raportează trebuie să furnizeze, în măsura în care este posibil, următoarele informații:

- natura încălcării descoperite
- gravitatea și amploarea încălcării

- categoriile de date vizate de încălcare
- numărul de persoane vizate afectate
- persoanele ce au avut acces la datele respective
- măsurile dispuse pentru limitarea efectelor încălcării

I.3. Investigarea incidentului

După ce a fost informat cu privire la un incident privind securitatea datelor, Responsabilul cu protecţia datelor, persoana cu atribuții sau conducerea, va întreprinde o scurtă investigaţie pentru a stabili dacă incidentul se confirmă sau nu.

Astfel, persoana care realizează investigația, va solicita furnizarea de detalii suplimentare părților care pot oferi aceste detalii, în termen de 24 de ore de la descoperirea încălcării, referitoare la:

- natura presupusei încălcări, inclusiv tipurile de date care au fost compromise şi modul în care se crede că a avut loc încălcarea potenţială a datelor
- cine este sau poate fi afectat, inclusiv numărul estimativ de persoane
- consecinţele încălcării şi ce măsuri pot fi luate sau care au fost luate pentru a diminua consecinţele încălcării

I.4. Informare şi notificare

Responsabilul cu protecţia datelor, persoana cu atribuții sau conducerea va fi responsabil(ă) de evaluarea încălcării şi de a recomanda Managementului decizia de a notifica încălcarea către autoritatea de supraveghere, în termen de 72 de ore de la momentul confirmării incidentului, pe *www.dataprotection.ro - https://www.dataprotection.ro/formulare/formularBresaGdpr.do?action=view_action&newFormular=true.*

Se va evalua totodată, dacă persoanele vizate trebuie să fie informate despre încălcare, iar dacă se constată necesar, se vor informa și persoanele vizate.

Responsabilul cu protecţia datelor sau persoana cu atribuții specifice, poate contacta, după cum este necesar, Secretariatul **[Operatorul]**, Poliţia dacă a existat o activitate ilegală, Managementul dacă este probabil să existe interes pentru presă, colaboratori IT&C dacă încălcarea implică şi securitatea IT, alte departamente, după caz. De asemenea, pot exista cerinţe legale sau contractuale de notificare.

I.5. Limitarea consecinţelor şi recuperarea

Persoanele însărcinate cu soluționarea incidentului privind securitatea datelor trebuie să ia cât mai curând posibil măsuri pentru a recupera pierderile şi limitarea daunele. Paşii sunt următorii:

- încercarea de recuperare a echipamentului pierdut
- încercarea de a restabili controlul asupra datelor personale, de exemplu rechemarea e-mail-urilor, eliminarea datelor de pe website-uri etc.
- utilizarea copiilor de siguranţă pentru a recupera datele pierdute, deteriorate sau furate, schimbarea parolelor relevante cât mai curând posibil
- dacă au fost pierdute / furate date bancare, contactarea directă a băncilor pentru sfaturi privind prevenirea utilizării frauduloase

I.6. Evaluare şi răspuns

Odată ce incidentul a fost ţinut sub control, persoanele însărcinate cu soluționarea incidentului trebuie să efectueze o analiză a cauzelor încălcării şi a eficacităţii răspunsului. Analiza trebuie să ia în considerare tipul de date, ce măsuri de protecţie au fost în vigoare (ex. criptarea), ce s-a întâmplat cu datele şi dacă ar putea exista consecinţe mai mari ale încălcării.

Dacă se identifică probleme în curs, atunci trebuie elaborat un **plan de acţiune** pentru a le pune în aplicare. În cazul celor mai grave încălcări, un raport va fi prezentat conducerii **[Operatorul]**.

Responsabilul cu protecţia datelor sau managementul unității medicale va ţine un **Registru de evidenţă a tuturor incidentelor** (excel) privind încălcarea confidenţialităţii datelor, inclusiv a acţiunilor întreprinse pentru a diminua consecinţele încălcării şi lecţiile învăţate.

Model Registru de evidență a incidentelor de securitate

Nr.	Tipul incidentului și modul în care a avut loc acesta	Caracterul încălcării securității datelor	Natura și conținutul datelor afectate de incident	Data și ora descoperirii	Data și ora survenirii	Persoana care a descoperit incidentul	Persoana responsabilă de domeniul în care a survenit incidentul	Gradul de probabilitate privind afectarea drepturilor persoanelor vizate	Măsurile luate anterior pentru prevenirea unui astfel de incident	Măsurile luate pentru a opri incidentul / ameliora situația	Necesitatea de a comunica incidentul Autorității Naționale / Persoanelor vizate	Numărul aproximativ și categoriile persoanelor vizate afectate	Consecințele probabile ale incidentului
1	Pierderea unui caiet (tip registru) care conținea numele, prenumele, numărul de telefon a 49 pontențiali clienți	Confidențialitate	Nume, prenume, oraș, telefon, sumă dorită, modalitate contract, observații	17.08.2022 ora 14:55	17.08.2022 ora 8:35	Angajatul operatorului cu atribuții specific pentru completarea registrului (caietului)	Managementul operatorului	Mic	1.Responsabilizarea angajaților prin menționarea unor prevederi cu titlu general în documente precum - Procedura de arhivare a documentelor, Regulamentul intern, convenția de confidențialitate semnată. 2. Scanarea documentului 3. Aprobarea unui plan de reacție la incidentele de securitate	Demararea unei investigații interne cu privire la incident. Contactarea firmei de curățenie / a celei de colectare a deșeurilor pentru încercarea de recuperare a documentelor . Informarea Responsabilului cu Protecția Datelor cu privire la incident.	Nu se impune, poate fi notificat dacă se decide în acest sens de către management	49 potențiali clienți ai operatorului	Contactarea persoanelor vizate în afara unui temei legal de către o persoană care recuperează părți din registru.

Calculul riscului

Informatii relevante	Proprietarii datelor	Tipul datelor	Detaliile riscului produs (Amenințări la confidențialitate, integritate, disponibilitate)	NOTĂ PROBABILITATE (1 - Mică, 10 - Mare)	NOTĂ GRAVITATE (1 - MICĂ, 10 - MARE)	SCORUL AMENINȚĂRII (2 - MICĂ, 20 - MARE)	Tratarea riscului (Tratează, Evită, Transferă sau Acceptă)	Data propusă pentru remedierea riscului	Data completării tabelului	Responsabilul riscului
				0	0	0				
				0	0	0				
				0	0	0				
				0	0	0				

Graficul riscurilor

		Impactul unui risc	Foarte mic	Mic	Mediu	Mare	Foarte mare
			ACCEPTABIL Efecte minime spre deloc		TOLERABIL Efectele sunt resimțite dar fără un rezultat critic	INDEZIRABIL Consecințe serioase asupra drepturilor persoanei vizate	INTOLERABIL Poate apărea un eveniment major (dezastru)
Probabilitatea producerii riscului	IMPROBABIL Este puțin posibil să apară riscul	Foarte mică	1	2	4	5	4
		Mică	2	3	5	6	7
	POSIBIL Este posibil ca riscul să apară	Medie	4	5	6	7	8
		Mare	5	6	7	8	9
	PROBABIL Riscul va apărea	Foarte mare	6	7	8	9	10