3.7 ORIENTĂRI CU PRIVIRE LA UTILIZAREA E-MAILULUI ȘI FAXULUI

- Prezentarea unora dintre riscurile și problematicile asociate utilizării e-mailului și faxului în contextul desfășurării activității medicale

- Identificarea aspectelor cheie care pot fi luate în considerare pentru a transmite date cu caracter personal prim e-mail sau fax

!NB - Medicii sunt responsabili cu reducerea riscurilor asociate comunicării prin e-mail sau fax și cu asigurarea măsurilor de protecție rezonabile pentru a proteja informațiile medicale personale.

Care sunt riscurile?

Orice comunicare cu pacientul prin intermediul e-mailului și faxului pentru a-i transmite informații medicale, respectiv date cu caracter personal, poate genera uneori efecte negative în ceea ce privește protejarea drepturilor pacientului. Acest lucru poate include dificultăți cu privire la confirmarea identității pacientului, a aparținătorilor, asupra confirmării stării de sănătate a pacienților sau poate chiar genera plângeri și acțiuni în justiție.

Exemplu: lipsa transmiterii unei scrisori medicale de transfer poate lipsi pacientul de posibilitatea de a beneficia în timp util de servicii medicale.

Astfel, putem identifica următoarele problematici:

Confirmarea identității pacientului / aparținătorului într-un e-mail sau fax primit

Exemplu: ne contactează pe email o persoană care se declară aparținătorul pacientului Dan Ioan, de pe o adresă de tipul pisycutza1989@yahoo.com

Exemplu: transmitem pe email niște rezultate medicale către un destinatar de tipul dan.ioan@gmail.com în loc să trimitem către un destinatar de tipul ioan.dan@gmail.com.

Folosirea unor emailuri personale în desfășurarea activității profesionale

Exemplu: Medicul Ionescu Andrei își pune la dispoziția pacienților adresa de email ionescu.andrei1989@yahoo.com pentru a-i comunica date cu privire la istoricul medical și diverse documente specifice în acest sens. Această adresă este mai apoi folosită în mod abuziv de un pacient care încearcă să îi vândă aparatură medicală medicului.

Putem identifica și următoarele riscuri pentru pacienți:

Consecințe negative asupra sănătății dacă este vorba de o problemă ce necesită consultație imediată și totuși există o întârziere în timpul de răspuns

Interpretarea eronată a conținutului unui e-mail sau al unui fax, ceea ce ar putea duce la:

- consecințe negative asupra sănătății
- plângeri
- acțiuni în justiție dacă percepția pacientului este una de comunicare inadecvată sau ineficientă.

Utilizarea e-mailului pentru a comunica cu pacienții sau cu furnizorii terți de servicii medicale poate da naștere la următoarele probleme de confidențialitate și securitate:

Un mesaj transmis prin e-mail care nu este criptat poate fi:

- interceptat de către terți neautorizați (ex. hackeri); A se avea în vedere încheierea de contracte de servicii de întreținere a sistemelor software prin care personalul cu pregătire IT vă poate oferi sprijinul necesar.

E-mailurile care conțin date cu caracter personal pot fi interceptate de terți neautorizați dacă e-mailul este:

- transmis către o adresă greșită;
- trimis sau primit din locații nesecurizate, cum ar fi cele accesibile publicului (ex. te afli într-un restaurant care are conexiune liberă Wifi)

Atașamentele dintr-un e-mail pot conține viruși care ar putea provoca daune grave sistemelor informatice

- **Exemplu**: Un atașament prin care se transmite o felicitare electronică cu ocazia sărbătorilor conține un virus care, odată ajuns pe dispozitivul dumneavoastră, blochează complet accesul la date.

Datele personale de sănătate trimise prin e-mail pot părăsi spațiul României sau al Uniunii Europene în timpul transmiterii și pot face obiectul legilor din alte jurisdicții care au protecții inadecvate sau nu au nicio protecție.

- **Exemplu**: În calitate de medic, dorești să consulți opinia medicală a unui fost coleg de facultate angajat al unui spital din S.U.A. În acest sens îi trimiți pe emailul de serviciu un email cu analizele medicale (ex. o radiografie) a unui pacient. Astfel se realizează un transfer de date în afara U.E. în lipsa unor măsuri tehnice și organizatorice adecvate.

Transmiterea prin fax a informațiilor personale de sănătate poate prezenta riscuri de confidențialitate și de securitate, deoarece informațiile personale pot fi accesate de terți neautorizați dacă faxul este:

- trimis la un număr de fax incorect (din cauza unei greșeli de apelare sau a apăsării unei taste de apelare rapidă greșite);
- expus persoanelor neautorizate din simplul motiv că faxul este amplasat într-o locație deschisă, nesecurizată; sau
- accesate de terți care interceptează sau monitorizează transmisia.

Cele mai bune practici

Măsuri care pot ajuta la protejarea e-mailurilor împotriva interceptării:

Folosirea unei conexiuni securizate la internet (HTTPS): Când accesați contul dvs. de e-mail sau când trimiteți sau primiți e-mailuri este important să utilizați o conexiune securizată la internet (HTTPS). Acest lucru poate fi verificat prin prezența unei **săgeți verzi** sau a unui **semn de încuietoare** în bara de adrese a browserului dvs.

- **Utilizarea exclusivă a conturilor profesionale,** e-mailurilor profesionale, dispozitivelor de servicii fax aparținând operatorului și care îl identifică pe operator, destinate în mod specific unor tipuri de comunicări.

- **Activarea autentificării în doi pași**: Autentificarea în doi pași presupune introducerea a două informații de autentificare pentru a accesa un cont, cum ar fi o parolă și un cod de verificare trimis prin SMS sau prin aplicație. Această măsură de siguranță adițională poate face mai greu pentru un atacator să acceseze contul dvs. de e-mail.

- **Utilizarea unui software anti-virus actualizat**: Un software anti-virus actualizat poate detecta și preveni instalarea de software malițios pe dispozitivul dvs., cum ar fi virusuri sau spyware care ar putea intercepta e-mailurile dvs.

- **Evitarea conectării la rețele Wi-Fi publice nesecurizate**: Conectarea la rețele Wi-Fi publice nesecurizate poate fi periculoasă, deoarece un atacator ar putea intercepta orice informație transmisă prin intermediul acestora, cum ar fi e-mailurile.

- **Folosirea parolelor puternice**: Parolele puternice sunt mai dificil de ghicit sau de spart decât parolele simple. Este important să utilizați parole puternice pentru conturile dvs. de e-mail și să le schimbați frecvent.

- **Evitarea deschiderii de fișiere atașate sau link-uri suspecte în e-mailuri:** E-mailurile sunt adesea utilizate pentru a răspândi malware sau pentru phishing. Este important să fiți precauți atunci când deschideți fișiere atașate sau link-uri în e-mailuri, mai ales dacă provin de la expeditori necunoscuți sau neașteptați.

Păstrarea e-mailurilor sau a documentelor transmise prin fax

Pentru păstrarea / salvarea e-mailurilor și faxurilor vă rugăm să aveți în vedere următoarele aspecte:

- Nu faceţi sau reţineţi mai multe copii ale comunicărilor prin email decât este necesar;
- Distrugeţi în siguranţă copii suplimentare care nu mai sunt necesare (pentru fax sau e-mailurile printate)

Cazuistică relevantă

Un exemplu problematic ar putea fi următorul:

La sfârșitul programului de muncă, doriți să trimiteți un email care cuprinde date cu caracter personal în conținutul acestuia dar și în atașament, date precum nume, prenume, boli asociate, diagnostic. Acest email ar trebui trimis către 2 destinatari. Funcția de autocompletare a emailului adaugă un alt destinatar cu nume similar decât cel relevant pentru dumneavoastră. Nu observați acest lucru și trimiteți emailul. Tocmai s-a realizat o divulgare de date neautorizată. Putem vorbi despre un incident care pune în pericol confidențialitatea datelor persoanei respective.

Pentru a evita astfel de incidente care pun în pericol confidențialitatea datelor cu caracter personal și se încadrează în categoria divulgării neautorizate, vă recomandăm următoarele măsuri:

- **Verificarea Destinatarilor**: Întotdeauna verificați cu atenție adresele de email ale destinatarilor înainte de a trimite un email. Aceasta este o etapă importantă, mai ales atunci când funcția de autocompletare a emailului este activată.
- **Setarea Confirmării de Trimitere**: Majoritatea clienților de email au o funcție care solicită o confirmare înainte de a trimite un email. Activarea acestei funcții vă poate ajuta să verificați din nou destinatarii și conținutul înainte de a trimite emailul.
- **Atașamentele Criptate**: Atunci când trimiteți informații sensibile ca atașamente, considerați utilizarea criptării (parolării) acestora. Acest lucru poate ajuta la prevenirea accesului neautorizat în cazul în care emailul este trimis greșit.
- **Educarea Personalului**: Asigurați-vă că toți membrii echipei dumneavoastră sunt conștienți de importanța securității datelor și cunosc cele mai bune practici pentru trimiterea emailurilor. O formare adecvată poate reduce semnificativ riscul de eroare umană.

Aceste măsuri, luate împreună, pot reduce semnificativ riscul unei divulgări neautorizate de date cu caracter personal. Cu toate acestea, este important să rețineți că nicio măsură de securitate nu este perfectă, iar atenția și vigilența constantă sunt esențiale pentru protejarea datelor.

Cazuistică din activitatea Autorității de Supraveghere:

În noiembrie 2022, Autoritatea Națională de Supraveghere a finalizat o investigație la Medicover S.R.L., constatând încălcarea articolelor 32(4), 32(1) (b) și 32(2) din GDPR. Ca urmare, operatorul a fost amendat cu 4.901 RON (aproximativ 1.000 de euro). Investigarea a început după ce Medicover a notificat autoritatea despre o încălcare a securității datelor, conform articolului 33 din GDPR. Încălcarea a avut loc când un e-mail conținând acte adiționale ale contractelor de prestări servicii medicale ale altor clienți a fost trimis unui client în mod eronat. Aceasta a dus la pierderea confidențialității datelor cu caracter personal, cum ar fi nume, CNP, adrese și semnături. Autoritatea a constatat că Medicover nu a implementat măsuri tehnice și organizatorice adecvate pentru a asigura un nivel corespunzător de confidențialitate și securitate, conform articolului 32 din GDPR.
Sursa:
https://www.dataprotection.ro/page=Comunicat_Presa_24_11_2022&lang=ro