

Securitate cibernetică și confidențialitatea datelor:

1. Conștientizarea riscurilor de securitate cibernetică:

a. Identificarea riscurilor:

- **Sensibilizarea la amenințări:** Informarea asupra amenințărilor cibernetice comune, cum ar fi malware, phishing, ransomware și atacuri de tip DDoS.
- **Cunoașterea surselor de vulnerabilitate:** Identificarea zonelor vulnerabile ale sistemului, inclusiv echipamente, rețele și dispozitive conectate la internet.

b. Educația privind tehnicile de atac:

- **Cunoașterea tacticilor utilizate:** Înțelegerea tehnicilor frecvent utilizate de hackeri și modul în care acestea pot afecta securitatea datelor.
- **Simularea atacurilor:** Organizarea de simulări de atac pentru a evalua nivelul de pregătire și răspuns al personalului.

2. Măsurile de securitate pentru protejarea datelor medicale sensibile:

a. Autentificare și controlul accesului:

- **Parole securizate:** Încurajarea utilizării de parole puternice și implementarea politicii de schimbare periodică a acestora.
- **Controlul accesului:** Asigurarea accesului restricționat la informații sensibile doar pentru personalul autorizat.

b. Criptarea datelor:

- **Utilizarea criptării:** Criptarea datelor în tranzit și în repaus pentru a preveni accesul neautorizat.
- **Certificarea protocolului HTTPS:** Asigurarea că toate conexiunile către platformele online sunt securizate prin protocolul HTTPS.

c. Actualizări și Patch-uri:

- **Politica de actualizare a Software-ului:** Implementarea unei politici de actualizare regulată a sistemelor și a software-ului pentru a remedia vulnerabilitățile cunoscute.
- **Monitorizarea Patch-urilor:** Monitorizarea și aplicarea rapidă a patch-urilor de securitate pentru a contracara amenințările cibernetice.

d. Backup și recuperare de date:

- **Backup regulat:** Realizarea de backup-uri periodice ale datelor critice și stocarea acestora într-un loc securizat.
- **Plan de recuperare a datelor:** Dezvoltarea unui plan de recuperare a datelor pentru a asigura recuperarea rapidă în caz de pierdere a datelor.

e. Politici și Proceduri de securitate:



- **Documentarea Politicilor:** Dezvoltarea și documentarea politicilor și procedurilor de securitate cibernetică.
- **Instruirea continuă:** Asigurarea formării continue pentru a menține personalul la curent cu cele mai recente amenințări și măsuri de securitate.

f. Monitorizarea activității și răspuns rapid:

- **Monitorizarea anomalii:** Implementarea unor sisteme de monitorizare a activității pentru a detecta rapid orice comportament neobișnuit.
- **Plan de răspuns la incidente:** Dezvoltarea unui plan de răspuns la incidente pentru a reacționa rapid în cazul unei vulnerabilități exploatare.

g. Consimțământ și educație a personalului:

- **Consimțământul informatic:** Obținerea consimțământului informatic al pacienților pentru colectarea și stocarea datelor lor.
- **Formare continuă a personalului:** Asigurarea unei formări continue pentru a crește conștientizarea personalului privind securitatea cibernetică și confidențialitatea datelor.

Implementarea acestor măsuri de securitate cibernetică asigură protejarea datelor medicale sensibile și menținerea unui mediu online sigur în cadrul clinicii.

Consultant introducere programe de formare

Patru Bogdan Adrian