10 Zasad Cyberbezpieczeństwa
dla Personelu Medycznego i Administracyjnego

Przekazanie kluczowych zasad bezpieczeństwa cyfrowego i ochrony danych pacjentów pracownikom placówek medycznych.

1 Nie otwieram podejrzanych e-maili ani załączników

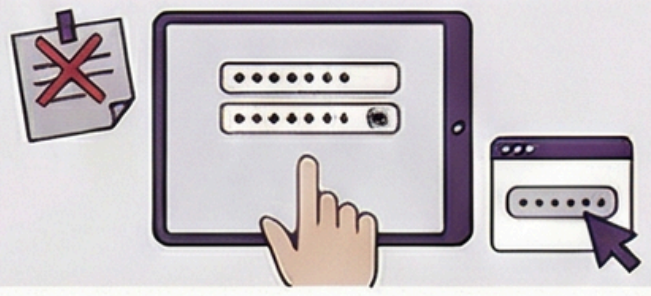
Jeśli wiadomość wzbudza wątpliwości (nieznany nadawca, presja czasu, prośba o dane lub kliknięcie linku), nie otwieram jej i zgłaszam ten fakt przełożonemu.

2 Zawsze blokuję komputer, gdy odchodzę od stanowiska

Nawet na chwilę. Zostawiony, odblokowany komputer to realne ryzyko naruszenia danych.

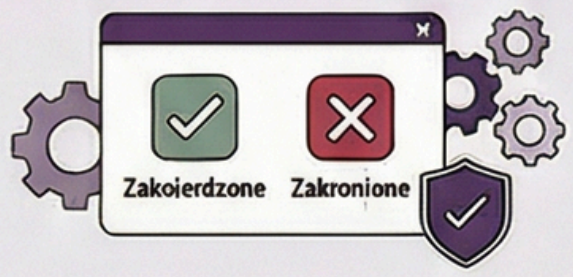
3 Nie udostępniam nikomu swoich loginów i haseł

Hasło jest indywidualne. Nie zapisuję go na kartkach, w notesach ani w przeglądarce.



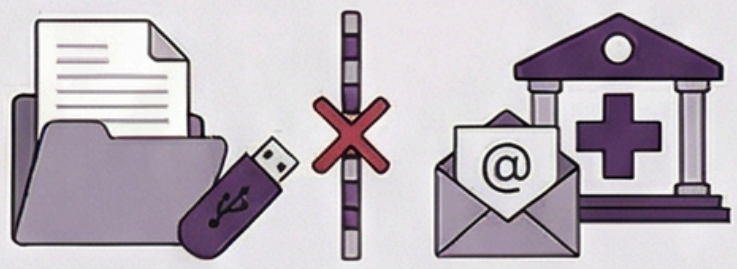
4 Korzystam wyłącznie z zatwierdzonego oprogramowania

Nie instaluję żadnych programów, aplikacji ani rozszerzeń bez zgody przełożonego.



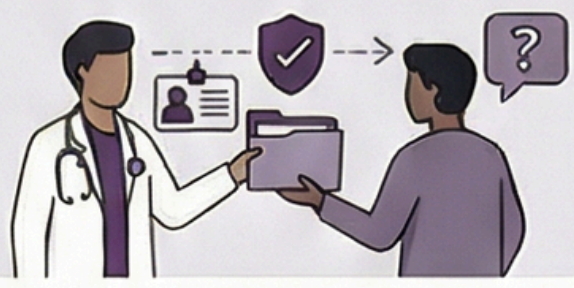
5 Nie wynoszę danych pacjentów poza placówkę

Dotyczy to zarówno dokumentów papierowych, jak i plików, zdjęć, pendrive'ów czy wysyłania danych na prywatne e-maile.



6 Sprawdzam, komu udostępniam informacje o pacjencie

Zanim przekażę jakiekolwiek dane, upewniam się, że rozmówca ma do tego prawo i jest właściwie zweryfikowany.

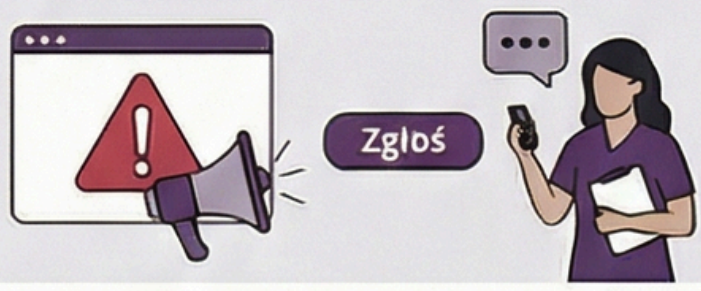


7 Nie korzystam z prywatnych nośników danych do pracy

Pendrive'y, dyski zewnętrzne czy karty pamięci mogą być używane tylko wtedy, gdy zostały dopuszczone przez placówkę.

8 Zgłaszam każdy incydent lub podejrzaną sytuację

Pomyłka, wysłanie maila do złego adresata, podejrzany e-mail - zgłaszam to od razu do IOD lub ADO.



9 Dbam o poufność rozmów i dokumentów

Nie omawiam danych pacjentów w miejscach publicznych, przy osobach trzecich ani przez nieautoryzowane kanały komunikacji.

10 Stosuję się do procedur i biorę udział w szkoleniach

Znam obowiązujące zasady bezpieczeństwa i stosuję je w codziennej pracy, nawet jeśli wydaję się „oczywiste". Biorę akrywny odział w szkoleniach z zakresu RODO i cyberbezpieczeństwa.