



Bezpieczeństwo teleporad i wideokonsultacji

w ramach zaleceń w zakresie podstaw
bezpieczeństwa i ochrony danych dla użytkowników
w sektorze ochrony zdrowia

01. Wybór odpowiedniego oprogramowania

- Korzystaj wyłącznie z zatwierdzonych przez placówkę platform do wideokonferencji. Powinny one gwarantować szyfrowane połączenia i zgodność z regulacjami dotyczącymi ochrony danych.
- Nie używaj do pracy prywatnych komunikatorów (np. WhatsApp, Messenger, Skype).
- Regularnie aktualizuj użytkowane oprogramowanie.
- Nie instaluj nieznanych aplikacji na urządzeniach służbowych. Używaj wyłącznie oficjalnych narzędzi rekomendowanych przez dział IT.
- Korzystaj z wersji biznesowych systemów lub platform medycznych, jeśli są dostępne (np. Microsoft Teams dla firm czy systemów dedykowanych dla telemedycyny).
- Nie próbuj na własną rękę instalować dodatkowych programów do poprawy jakości połączeń. Mogą one naruszać bezpieczeństwo systemów.

02. Zapewnienie prywatności rozmów

- Przeprowadzaj teleporady i wideokonsultacje w pomieszczeniu bez osób postronnych.
- Używaj słuchawek, aby zapobiec przypadkowemu podsłuchowi, szczególnie w miejscach, gdzie znajdują się inni pracownicy lub domownicy.
- Z wyprzedzeniem ustal, czy rozmowa może być nagrywana i na jakich warunkach. Nagrania powinny być przechowywane zgodnie z polityką placówki.
- Zamykaj okna i drzwi w trakcie konsultacji. Minimalizuje to ryzyko naruszenia prywatności pacjenta.
- Unikaj przeprowadzania teleporad w miejscach publicznych – kawiarnie, pociągi czy poczekalnie nie są odpowiednimi miejscami do omawiania poufnych informacji pacjentów.
- Nie używaj publicznych sieci Wi-Fi do przeprowadzania teleporad.

03. Weryfikacja pacjenta lub rozmówcy

- Zachowaj ostrożność, jeśli pacjent łączy się z nieznanego numeru lub adresu e-mail. Jeśli masz wątpliwości, potwierdź jego tożsamość innym kanałem.
- Nie podawaj wrażliwych informacji, dopóki nie potwierdzisz tożsamości rozmówcy. Nawet jeśli ktoś twierdzi, że jest pacjentem lub współpracownikiem.
- Przed rozpoczęciem konsultacji potwierdź tożsamość rozmówcy np. poprzez podanie numeru PESEL, daty urodzenia lub innego unikalnego identyfikatora.
- Nie udostępniaj pacjentowi lub klientowi jego własnych danych w celu potwierdzenia tożsamości. To pacjent powinien podać swoje dane w celu weryfikacji.
- Uważaj na przypadki podszywania się pod pacjentów (tzw. vishing). Jeśli rozmówca zachowuje się podejrzanie lub nie jest w stanie podać poprawnych danych, rozważ zakończenie rozmowy i skontaktowanie się z nim innym sposobem.
- Jeśli pacjent chce, aby inna osoba uczestniczyła w rozmowie, wymagana jest jego wyraźna zgoda. Najlepiej zapisana w dokumentacji medycznej i potwierdzona przez pacjenta na piśmie.
- Nie udostępniaj informacji medycznych osobom nieupoważnionym.

04. Bezpieczne przechowywanie dokumentacji z teleporad

- Przetwarzaj informacje z teleporady tak, jak w przypadku tradycyjnej wizyty, zachowując zgodność z przepisami i wewnętrznymi procedurami placówki.
- Nie przechowuj nagrań i dokumentów na prywatnym komputerze lub telefonie. Dane medyczne i służbowe muszą być archiwizowane w zatwierdzonych systemach.
- Korzystaj wyłącznie z firmowych systemów do przechowywania danych.
- Regularnie sprawdzaj uprawnienia dostępu do dokumentacji. Upewnij się, że tylko uprawnione osoby mają do niej dostęp.
- Nie udostępniaj raportów z wideokonsultacji przez niezabezpieczone kanały np. prywatne e-maile, niezaufane chmury czy komunikatory.