

Cyberbezpieczeństwo w pracy gabinetowej – na co zwrócić uwagę przy zdalnym udzielaniu pomocy

mgr inż. Angelika Maria Piątkowska,
Fundacja Polski Instytut Cyberpsychologii,
Cyberpsychopatologii i Cyberpsychotraumatologii



Co ja za jedna



Programistka .NET w BCF Software



Studentka na WSB-NLU (psychologia,
psychotraumatologia z elementami suicydologii) i
wykładam (cyberpsychologia)



Prezes Polskim Instytucie Cyberpsychologii,
Cyberpsychopatologii i Cyberpsychotraumatologii



Praktykantka w psychodzy24.pl



Wołchwyni w Rodzimym Kościele Polskim



Mrówczarka



Ircowniczka (#listekklonu@irc.pirc.pl)

Disclaimer



To co mówię, to mówię ja i jest to mój prywatny punkt widzenia – a nie stanowisko żadnego z podmiotów wymienionych na poprzednim slajdzie (ani żadnych pozostałych)



W trakcie prezentacji będę używać formy „per ty”.

O czym będzie

Dlaczego cyberbezpieczeństwo w gabinecie online jest aż tak kluczowe?

Poufność

Hasła

RODO

Bezpieczne metody komunikacji

Środowisko pracy

Cyberbezpieczeństwo - elementy

Dlaczego cyberbezpieczeństwo w gabinecie online jest aż tak kluczowe?



Tajemnica zawodowa

Poufność
Zaufanie – fundament relacji



Dane szczególnie
wrażliwe

Etyka zawodowa
Ochrona prawna



Cel ataku

Nikt nie jest za mały np. na
ransomware
Czasami to kwestia zwykłej
kradzieży (online czy offline)



Konsekwencje

Reputacyjne
Finansowe (i prawne)

Modele pracy zdalnej

-
- Wideo (synchronicznie) – najczęstsza forma
 - Audio/telefon – mniejsza ekspozycja wizualna
 - Czat tekstowy – zapis rozmowy jako dane
 - E-mail/asynchronicznie – ryzyko przecieku
 - Hybrydy (np. spotkanie video + bezpieczna wymiana plików)

Formy wsparcia psychologicznego online są bardzo różne, a powyższe formy nie wyczerpują możliwości.



Jak zadbać o poufność

Poza NFZ nie mamy obowiązku przechowywania jakichkolwiek danych personalnych, możemy sobie dowolnie kodować notatki i nie trzymać kartotek

Zbierajmy tylko te dane, które są nam niezbędne - im mniej tym lepiej.

Poufność otoczenia po obu stronach (słuchawki, drzwi)

Brak osób trzecich (chyba że jest wyraźna zgoda obu stron)

NIE NAGRYWAMY (chyba że za obopólną zgodą do konkretnych celów - np. superwizja)

Korzystamy z szyfrowania na każdym możliwym poziomie.

Mit zielonej kłódki

Co oznacza
(oznaczała)
zielona
kłódeczka?

Przed czym
chroni, a przed
czym nie?

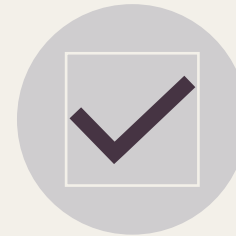
O co chodzi z
tymi
certyfikatami?



A co z hasłami?



MANAGERY HASEŁ



UWIERZYTELNIANIE
WIEŁOSKŁADNIKOWE



NIEPOWTARZAJĄCE
SIĘ HASŁA



DŁUGIE HASŁO-
MATKA



KAŻDY SVOJE



NIGDY MAILEM

<https://www.youtube.com/watch?v=CmeTFbennLU> –

tutaj o uwierzytelnianiu dwuskładnikowym (można składników dodać)

Uwierzytelnianie wieloskładnikowe (MFA)



Aplikacja TOTP zamiast SMS, klucze sprzętowe tam, gdzie możliwe



MFA dla: e-mail, chmura, kalendarz, wideoplatforma



Kody awaryjne – bezpieczne przechowywanie



Edukacja dot. ataków MFA-fatigue



Wyłączenie MFA tylko w wyjątkowych sytuacjach (czasowo)

Sieć domowa i VPN



SILNE HASŁO WI-FI,
WPA2/3, UKRYWANIE SSID
ZBĘDNE



ODDZIELNA SIEĆ DLA
GOŚCI/URZĄDZEŃ IOT



AKTUALIZACJE ROUTERA,
ZMIANA DOMYŚLNEGO
HASŁA ADMIN



VPN DO ZASOBÓW
GABINETU/CHMURY (JEŚLI
WYMAGANE)



MONITOROWANIE
NIEZNANYCH URZĄDZEŃ
W SIECI



Bezpieczne metody komunikacji w otwartym Internecie



Session (ale trudny w użytku)



Signal



Telegram (ale tylko szyfrowane)



WhatsApp (ale uwaga na pegazusa)



Messenger (OSTATECZNOŚĆ - od niedawna ma szyfrowanie)

I ustawiaj samoniszczące się wiadomości!

Plan bezpieczeństwa i kryzysy

Procedura na: ryzyko samobójcze, przemoc,
nagłe pogorszenie

Zbieranie informacji lokalizacyjnych klienta
przed sesją

Lista numerów alarmowych, telefonów
zaufania, miejsc, gdzie można uzyskać
wsparcie

Zgoda na kontakt z osobą trzecią w nagłych
wypadkach

Dokumentacja interwencji i powiadomień

Weryfikacja tożsamości klienta online

- Imię i nazwisko + data urodzenia + kontakt awaryjny
- Potwierdzenie lokalizacji przed sesją (adres do interwencji)
- Zgody opiekuna prawnego w pracy z nieletnimi
- Ustal sposób szybkiej weryfikacji w kryzysie
- Bez przechowywania skanów dokumentów bez konieczności



RODO – Obowiązuje nas



Jeżeli nie przewidujemy anonimowego udzielania pomocy – to przetwarzamy dane osobowe – chociażby po to, by kogoś zarejestrować na konkretną godzinę. Jesteśmy więc administratorami przetwarzającymi dane osobowe w kontekście RODO. Chyba że jesteśmy zatrudnieni w jakiejś sieciówce, wtedy to ona za to odpowiada, a my podpisujemy z nimi stosowne umowy.



Klauzula informacyjna / Polityka prywatności (art. 13/14 RODO) – komu, po co, na jakiej podstawie, jak długo, komu ujawniasz, prawa osoby, kontakt. Koniecznie daj do podpisania na pierwszej wizycie! Możesz udostępnić te dokumenty do zapoznania się elektronicznie z możliwością odklikania zapoznania się z tymi dokumentami.

Role i odpowiedzialności



Administrator danych: gabinet/praktyka



Podmiot przetwarzający: dostawcy narzędzi (np. wideoplatforma)



Współadministratorzy - gdy współdecydujecie o celach/środkach



Upoważnienia, zakresy obowiązków i szkolenia personelu



Rejestr czynności przetwarzania ROPA (co, po co, jak długo, opis procesów (rejestracja, konsultacja online, fakturowanie))

<https://gdpr-text.com/pl/read/article-32/>

Artykuł 32 RODO. Bezpieczeństwo przetwarzania

1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:

↳ Wytyczne & Case Law ▼

a) pseudonimizację i szyfrowanie danych osobowych;

↳ ISO 27701 ▼

b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;

↳ ISO 2

c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;

↳ ISO 2

d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

↳ ISO 2

Co to znaczy, że dane są bezpieczne?

Poufność

- Tylko ci, co mają mieć dostęp – mają go – i nikt inny

Integralność

- Nikt i nic nie wpłynęło na dane

Dostępność

- Uprawnieni mogą bez problemu się dostać do danych

Autentyczność

- Mamy pewność kto nam te dane daje (lub kto daną czynność wykonuje)

Rozliczalność

- Wiemy kto co i kiedy robił (na jakichś danych, w jakimś systemie)

Niezawodność

- Wiemy, że nic się nie zepsuje

Niezaprzeczalność

- Autor nie ma jak się autorstwa wyprzeć

***Ale ja żadnych danych nie przetwarzam!
Mam od tego ludzi!***

Świetnie. A masz z nimi podpisane Umowy powierzenia danych (DPA)?

- Obsługa IT (w tym serwis)
- Webmaster, marketing, social media, PR
- Platformy video, rejestracyjne, kartotekowe
- Usługi chmurowe, poczta elektroniczna, kalendarze
- Księgowość, obsługa płatności

Dowiedz się jak to zrobić i uzupełnij papierologię.

Współpraca i przekazywanie danych



NAJMNIEJ
KONIECZNY ZAKRES
(DATA MINIMIZATION)



SZYFROWANIE ORAZ
KONTROLA ODBIORU



UMOWY I PODSTAWY
PRAWNE
PRZEKAZANIA



WERYFIKACJA
TOŻSAMOŚCI
PARTNERA/INSTYTUCJI



REJESTR
UDOSTĘPNIENÍ

Umowy powierzenia (DPA) – co sprawdzić



Zakres, kategorie danych i cele przetwarzania



Miejsce przetwarzania (UE/EOG, transfery poza EOG)



Środki techniczne i organizacyjne dostawcy



Podpowierzenie i audyty



Procedury incydentowe i usuwanie danych po zakończeniu

Kiedy DPIA (Ocena Skutków dla Ochrony Danych) jest obowiązkowa?

Kryterium	☐ TAK ☐ NIE	Uzasadnienie (krótko)
Dane szczególnych kategorii (zdrowotne, psychologiczne) - przetwarzanie systematyczne.	☐ TAK ☐ NIE	
Osoby w sytuacji wrażliwej (dzieci, osoby w kryzysie, pacjenci).	☐ TAK ☐ NIE	
Duża skala przetwarzania (liczba osób, zakres danych, czas trwania, geografia).	☐ TAK ☐ NIE	
Łączenie/porównywanie zbiorów z różnych źródeł (EHR + ankiety + narzędzia analityczne).	☐ TAK ☐ NIE	
Innowacyjna technologia (np. automatyczna transkrypcja/AI w chmurze).	☐ TAK ☐ NIE	
Transfer danych poza EOG lub do państwa bez decyzji adekwatności; złożony łańcuch podpowierzeń.	☐ TAK ☐ NIE	
Długotrwałe, systematyczne przetwarzanie/monitorowanie zachowań (np. rozbudowane logi).	☐ TAK ☐ NIE	
Profilowanie/ocena z konsekwencjami (dostęp do usługi, kategoryzacja ryzyka).	☐ TAK ☐ NIE	
Dane lokalizacyjne, finansowe lub inne o podwyższonym ryzyku nadużycia.	☐ TAK ☐ NIE	

Min 2

Inne dokumenty, które trzeba mieć

- Rejestr naruszeń + procedura incydentowa
- **Upoważnienia do przetwarzania + ewidencja osób upoważnionych** (dla współpracowników/asysty) + oświadczenia poufności.
- Decyzja nt. wyznaczenia IOD (inspektora) lub uzasadnienie braku obowiązku
- Regulamin świadczenia usług drogą elektroniczną (UŚUDE)
- Polityka Cookies
- **Zgody operacyjne:**
 - zgoda na **formę zdalną** (ryzyka/ograniczenia),
 - zgoda **opiekuna** przy nieletnich,
 - zgoda na **nagrywanie** (jeśli w ogóle),
 - zgoda marketingowa (jeśli używasz).

***Możliwe, że
potrzebujesz też
coś z tego***



Polityka retencji i bezpiecznego usuwania (z harmonogramem).



Plan ciągłości działania/odtworzenia (BCP/DR) + testy kopii 3-2-1.



Polityki IT: dostępów/hasel/MFA, BYOD/praca zdalna, szyfrowanie dysków, backup, zarządzanie łatkami.



Procedura transferów poza EOG + ocena TIA/SCC (jeśli korzystasz).



Procedura korzystania z narzędzi AI (bez danych identyfikujących).



Rejestr udostępnień danych (np. do ubezpieczycieli, sądów, szkół).



Wzorcowe formularze: zgody (tele, nagrywanie, opiekun), NDA dla podwykonawców, DPA (um. O powierzenie danych) dla dostawców.



Szkolenia i rejestr szkoleń (phishing, ochrona danych).

3-2-1-0 Backupik 😊

Zasada kopii 3-2-1

Prosty sposób, aby dane gabinetu przetrwały awarie i ransomware

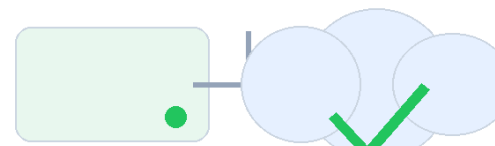
3 kopie danych



1 robocza + 2 zapasowe

Jeśli jedna kopia zginie lub zostanie zaszyfrowana, wciąż masz dwie zapasowe do odtworzenia.

2 różne nośniki



np. dysk + chmura/NAS

Różne technologie =
mniejsze ryzyko wspólnej
awarii.

1 kopia poza siedzibą



off-site: chmura w UE/EOG lub odłączony dysk w innym miejscu

Chroni przed
kradzieżą/pożarem oraz
skutkami lokalnych awarii.

Wersja wzmocniona: 3-2-1-1-0

Dodatkowo: 1 kopia niemutowalna/offline + 0 błędów w testowym odtwarzaniu

Nagrywanie sesji – polityka i ryzyka

Domyślnie: nie
nagrywać, jeśli nie
ma silnej potrzeby

Jeśli nagrywasz: cel,
zgoda, retencja,
bezpieczne
przechowywanie

Ryzyko wycieku po
stronie klienta

Alternatywy:
notatki, transkrypcje
lokalne bez chmury

Transparentna
komunikacja i
zgody na piśmie

Zgody zgody zgody...



Podstawa prawna świadczenia usługi



Zgoda poinformowana na formę zdalną
(ryzyka, ograniczenia)



Wycofanie zgody – jasna procedura



Zgoda na nagrywanie/udostępnianie
materiałów (jeśli dotyczy)



Odnotowanie zgód i podstaw w dokumentacji

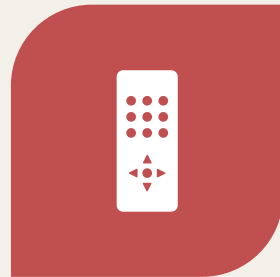
Nieletni i zgody opiekuna



WERYFIKACJA PRAWNEGO
OPIEKUNA I
DOKUMENTACJA ZGODY



USTALANIE OBECNOŚCI
OPIEKUNA PODCZAS SESJI
(KIEDY I JAK)



KANAŁY KONTAKTU W
KRYZYSIE (SZKOŁA,
KURATOR, OPS)



KOMUNIKACJA ADEKWATNA
DO WIEKU, PRYWATNOŚĆ
NASTOLATKA



PRZECHOWYWANIE I
UDOSTĘPNIANIE NOTATEK –
SZCZEGÓLNA OSTROŻNOŚĆ

Udzielanie pomocy zdalnie cudzoziemcom

Ustalenie jurysdykcji i wymogów
lokalnych klienta

Różnice w numerach alarmowych
i zasobach kryzysowych

Transfer danych poza EOG –
ocena i zabezpieczenia

Kwestie licencji zawodowych w
innych krajach (jeśli dotyczy)

Jasne warunki świadczenia usług
w regulaminie

Minimalizacja i retencja danych

- Projektuj formularze tak, by nie zbierały nadmiaru
- Ustal polityki retencji (jak długo, gdzie, kto)
- Anonimizacja/de-identyfikacja, gdy to możliwe
- Bezpieczne usuwanie (w tym kopii i urządzeń)
- Regularne przeglądy zbiorów danych



Prawa klientów/pacjentów



Dostęp do danych, sprostowanie,
ograniczenie przetwarzania



Przenoszenie i sprzeciw – jak je obsługiwać



Wgląd do logów dostępu (jeśli prowadzisz)



Przygotowane szablony odpowiedzi i
weryfikacja tożsamości



Terminy i dokumentowanie obsługi
wniosków

Środowisko pracy – prywatność i akustyka



Oddzielne pomieszczenie, zamykane drzwi, biały szum



Słuchawki nauszne, kamera ustawiona na neutralne tło (albo wybrać tło)



Oznaczenia na drzwiach (nie przeszkadzać)



Porządek na biurku i pulpicie (widoczne pliki)

Urządzenia

Sprzęt służbowy
oddzielony od
prywatnego

Ekran prywatności,
blokada ekranu,
automatyczne
uśpienie

Antywirus/EDR

Regularny serwis i
inwentaryzacja

Nośniki wymienne
- polityka użycia
lub zakaz

Aktualizacje i łatki



SYSTEM OPERACYJNY I
OPROGRAMOWANIE -
AUTOMATYCZNE
AKTUALIZACJE



AKTUALNE PRZEGLĄDARKI I
WTYCZKI



WYŁĄCZANIE ZBĘDNYCH
USŁUG



MONITOROWANIE EOL
(KONIEC WSPARCIA) SPRZĘTU
I OPROGRAMOWANIA



TESTY PO AKTUALIZACJACH
KRYTYCZNYCH

Obowiązuje nas tajemnica zawodowa.

Nie wiemy do czego firmy trzecie wykorzystają nasze rozmowy z pacjentem-klientem czy innymi osobami.

Nie wiemy jak zostaną wykorzystane dane osobowe czy medyczne.

Nie używajmy.

W te miejsca powinny trafiać tylko dane, które mogą być traktowane jako publiczne

Możemy wykorzystywać te zdobycze technologii w naszej pracy, ale NIE KARMIMY ich informacjami o pacjentach-klientach

***Na co
uważać***

Sztuczna
inteligencja

Boty do
transkrypcji
rozmów

Boty do
podsumowania
spotkań

Usługi
chmurowe

Chmura

Twoje dane
gdzieś oddane



Kartoteki, notatki z terapii, dane osobowe
NIE POWINNY TRAFIAĆ DO CHMURY





*Chyba że
zaszyfrowane*

Co szyfrować?

Pliki z danymi
wrażliwymi i
osobowymi

Całe dyski (lub
dyski wirtualne)

Wszystko, co
wysyłamy do
chmur

Całe urządzenia
przenośne
(laptopy,
smartfony)

Pendrive'y, dyski
przenośne

Kopie zapasowe



Jak szyfrować?

- Szyfrowanie pełnodyskowe (BitLocker, FileVault, LUKS)
- Szyfrowane foldery/archiwa dla dokumentów wrażliwych
- Menadżer kluczy i polityka odzyskiwania
- Szyfrowanie urządzeń mobilnych i kopii zapasowych
- Higiena haseł do archiwów i kluczy



Co można bezpiecznie wrzucić do chmury



Szablony dokumentów
(„puste” dokumenty)



Grafikę służbową (loga
poradni, papeterię
firmową)



Narzędzia
wykorzystywane w pracy
(karty prac, tabelki, bazy
pytań)



Regulaminy, karty
charakterystyk,
wewnętrzne procedury



Arkusze z zestawieniami
wewnątrzfirmowymi



Wszystkie dane
powiązane z pacjentem-
klientem dopiero po ich
zaszyfrowaniu

Nie rezygnujemy zupełnie! Korzystamy z głową!

Bezpieczna wymiana plików



Nie wysyłaj danych wrażliwych zwykłym e-mailem



Używaj szyfrowanych łączy do pobrania z limitem czasu



Hasła kanałem alternatywnym (telefon/SMS/TOTP)



Ogranicz dostęp do trybu tylko-do-odczytu



Śledzenie udostępnień i odwoływanie linków

Poczta elektroniczna

S/MIME lub PGP – gdy wymagana korespondencja wrażliwa

Filtry anty-spam i ostrzeżenia przed zewnętrznymi nadawcami

Unikaj autosugestii adresów – błąd odbiorcy = wyciek

Stopka poufności + wskazówka szyfrowania

MFA

Phishing i socjotechnika



ROZPOZNAWANIE
FAŁSZYWYCH LINKÓW I
ZAŁĄCZNIKÓW



WERYFIKACJA PROŚB O
PŁATNOŚĆ/ZMIANĘ
KONTA



OSTRZEŻENIA W
PRZEGLĄDARCE I
SANDBOX
ZAŁĄCZNIKÓW

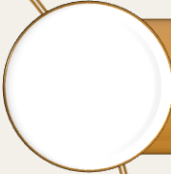
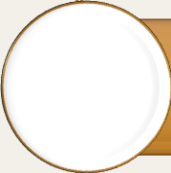
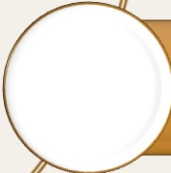


ZASADA: WĄTPLIWOŚCI
→ INNY KANAŁ,
ODDZWOŃ



SZKOLENIA I
SYMULACJE
PHISHINGOWE (W
ZESPOLE)

Do czego wykorzystywać AI

-  Tworzenie narzędzi terapeutycznych
-  Tworzenie czytanek, bajek terapeutycznych
-  Tworzenie grafik



Do czego nie wykorzystywać AI



Tworzenie streszczeń z rozmów z pacjentem-klientem



Tworzenie dokumentacji medycznych, opinii psychologicznych



Tworzenie deep fake'ów z wykorzystaniem czyjegoś głosu lub wizerunku



CHYBA ŻE DOTYCZY TO ZANONIMIZOWANEGO PRZYPADKU DO CELÓW EDUKACYJNYCH

Scenariusze i case studies

- Zgubiony laptop z notatkami – co robisz?
- Klient rozsyła nagranie sesji – reakcja
- E-mail z „pilną zmianą” nr konta – weryfikacja
- Atak ransomware na dysk gabinetu – odtwarzanie
- Praca z klientem za granicą – ustalenie jurysdykcji



Instytut_Cyberpsychologii_15



***Jakie macie
pytania?***



Kontakt do mnie

PIATKOSIA.APT@INTERIA.PL, PIATKOSIA@CYBERPSYCHOINSTITUT.PL

<https://twitter.com/piatkosia>

PIATKOSIA (IRC.PIRC.PL)

<https://github.com/Piatkosia>

<https://www.linkedin.com/in/piatkosia/>

Telefon/Signal/Telegram : 726 713 162

GG 12704498☺



- **Dziękuję za uwagę**