Co się dzieje z moimi danymi i danymi moich pacjentów?

Wersja dokumentu: 1.0 · **Dotyczy paniAnetki w wersji v5+ Język:** polski

---

To jest pytanie, które każdy lekarz powinien sobie zadać przed zainstalowaniem oprogramowania. Ten dokument odpowiada na nie **bez branżowego żargonu**.

W skrócie: **paniAnetka działa w całości na Twoim komputerze**. Żadne nagrania ani treści raportów nie są wysyłane do internetu. Niżej tłumaczymy szczegółowo — gdzie są dane, co je opuszcza komputer (mało), jak je zabezpieczyć i jakie są **ograniczenia, o których powinieneś wiedzieć**.

---

1. Trzy rodzaje danych

W trakcie pracy z paniAnetką powstają trzy rodzaje danych:

Rodzaj	Przykład	Gdzie żyje
Dane Twoich pacjentów	imię, PESEL, opis badania, nagranie, raport	Tylko na Twoim komputerze
Twoje dane jako lekarza	imię, PWZ, email, klucz licencyjny	Na Twoim komputerze + serwer licencyjny
Dane techniczne	wersja aplikacji, błędy, wydajność	Tylko na Twoim komputerze (chyba że włączysz telemetrię)

Każdy z nich ma inne reguły. Omówię osobno.

---

2. Dane pacjentów — w pełni offline

Co to jest

Wszystko, co dotyczy konkretnego pacjenta:

- Imię, nazwisko, PESEL, telefon
- Twoje **nagranie głosu** (kilkadziesiąt sekund do kilku minut)
- **Transkrypcja** — to, co powiedziałeś, zapisane jako tekst

- **Raport** — gotowy dokument PDF/DOCX
- Historia poprzednich wizyt tego pacjenta

Gdzie to się fizycznie znajduje

Wszystko zapisane na **dysku Twojego komputera**, w folderze ukrytym przed zwykłym widokiem:

- **macOS:** `~/Library/Application Support/PaniAnetka/historia/historia.db`
- **Windows:** `%APPDATA%\PaniAnetka\historia\historia.db`

To pojedynczy plik bazy danych (`.db`). Nikt poza Tobą do niego nie ma dostępu — chyba że ktoś inny zaloguje się na Twoje konto użytkownika.

Co NIE wychodzi z Twojego komputera

- ❌ Nagrania głosowe — nigdy nie opuszczają komputera
- ❌ Transkrypcje — nigdy nie opuszczają komputera
- ❌ Raporty — nigdy nie opuszczają komputera (jeśli sam ich nie wyślesz)
- ❌ PESEL, imię i nazwisko pacjenta — nigdy nie opuszczają komputera

Dlaczego można nam wierzyć? Ponieważ paniAnetka **nie korzysta z chmury AI** (jak ChatGPT czy Google). Modele Whisper (rozpoznawanie mowy) i model językowy (formatowanie raportu) są **uruchamiane bezpośrednio na Twoim komputerze** — to one zużywają RAM i są powodem, dla którego potrzebujesz 16 GB pamięci.

> Możesz to sprawdzić sam: wyłącz internet (Wi-Fi off) — paniAnetka nadal będzie nagrywać, transkrybować i generować raporty. Internet potrzebny jest tylko do **pierwszej aktywacji licencji** i sprawdzania aktualizacji.

---

3. Twoje dane jako lekarza

Co to jest

- Twoje imię, nazwisko, tytuł, specjalność, PWZ
- Adres gabinetu, telefon
- Email (jeśli podałeś podczas zakupu)
- Klucz licencyjny aplikacji
- Tzw. "fingerprint maszyny" — anonimowy identyfikator Twojego komputera (do weryfikacji licencji)

Co i kiedy wychodzi z komputera

- **Raz, podczas aktywacji licencji** — Twój klucz licencyjny + fingerprint maszyny są przesyłane do naszego serwera, by potwierdzić, że masz prawo używać aplikacji. **Nie przesyłamy** tu Twoich danych pacjentów, raportów, nagrań.
- **Raz w tygodniu** — aplikacja sprawdza czy Twoja licencja jest nadal ważna (anti-piracy). Wymiana to tylko fingerprint + status.
- **Sprawdzanie aktualizacji** — przy starcie aplikacji pytamy serwer „jest nowsza wersja?". Nie wysyłamy w tym żadnych danych poza wersją Twojej aplikacji.

Gdzie to leży

Po Twojej stronie:

- Twoje dane lekarskie: `~/Library/Application Support/PaniAnetka/config.json` (macOS) lub odpowiednik na Windows.
- Klucz licencyjny: `~/.../PaniAnetka/license.json` + dodatkowa kopia w macOS Keychain / Windows Credential Manager.

Po naszej stronie (na serwerze panianetka.pl):

- Klucz licencyjny ↔ Twój email i imię (do faktur i kontaktu)
- Historia aktywacji (kiedy i z jakiego fingerprintu maszyny)
- **NIC więcej.** Nie mamy dostępu do Twoich pacjentów, nagrań, raportów.

---

4. Dane techniczne — opt-in

Czym jest „anonimowa telemetria"

paniAnetka może wysyłać do nas **anonimowe metryki techniczne**, które pomagają nam łapać błędy i poprawiać jakość modeli AI:

- Czas transkrypcji (np. „nagranie 60 s zostało przetłumaczone w 12 s")
- Czas generowania raportu
- Wersja aplikacji, model AI, system operacyjny (macOS/Windows)
- Anonimowy UUID instalacji (zlepek liczb i liter, **nie jest powiązany z Twoim PWZ ani imieniem**)
- Komunikaty błędów (np. „brakuje pamięci RAM")

Czego nie wysyłamy w telemetrii

- ❌ Treści nagrań ani transkrypcji
- ❌ Treści raportów
- ❌ Imienia, nazwiska, PESEL pacjenta

- ❌ Twojego imienia, PWZ, emaila
- ❌ Niczego, co pozwoliłoby zidentyfikować pacjenta lub Ciebie

Jak wyłączyć

- W **Wizardzie pierwszego uruchomienia**, krok 8 — odznacz checkbox „Anonimowa telemetria"
- W **Ustawieniach** → 🔒 **Prywatność** → **Telemetria** w każdej chwili

Telemetria jest **w 100% opcjonalna** i nie wpływa na działanie aplikacji.

---

5. Co powinieneś zrobić, żeby zabezpieczyć dane pacjentów

paniAnetka chroni dane „w locie" (na czas pracy z aplikacją), ale **plik `historia.db` na Twoim dysku** jest tak bezpieczny, jak zabezpieczony jest sam komputer. Jako administrator danych pacjentów odpowiadasz za ich ochronę.

Krytyczne minimum (zrób to dziś)

1. **Hasło użytkownika na komputerze** — silne, niepowtarzalne. Bez tego każdy, kto fizycznie usiądzie przy Twoim Macu/PC, zobaczy historię pacjentów.
2. **Pełnoekranowe szyfrowanie dysku:**
   - **macOS: FileVault** — Ustawienia systemowe → Prywatność i bezpieczeństwo → FileVault → Włącz. Po godzinie cały dysk jest zaszyfrowany. Bez Twojego hasła **nie da się** odczytać żadnego pliku, nawet wyjmując dysk z komputera.
   - **Windows: BitLocker** (Pro/Enterprise) lub Device Encryption (Home) — Ustawienia → System → Informacje → Szyfrowanie urządzenia
3. **Automatyczna blokada ekranu** po 5 minutach bezczynności — w gabinecie kompromis nie do uniknięcia.

Dobry standard

4. **Backup `historia.db`** — przynajmniej raz w tygodniu skopiuj plik na zewnętrzny dysk lub szyfrowaną pamięć USB. **Nie używaj iCloud/Google Drive/Dropboxa** — to wysyła dane pacjentów do chmury.
5. **Gdy zmieniasz komputer** — `historia.db` (i cały folder `PaniAnetka/`) skopiuj na nowy komputer. Stary komputer **wykasuj** (Disk Utility → Erase, Windows: Reset PC + secure erase).
6. **Praca w gabinecie** — nie pozwalaj na pracę pacjenta/recepcjonistki na Twoim koncie użytkownika. Każdy ma własne konto.

Wyższy standard (Pro)

7. **Osobny komputer tylko do pracy medycznej** — bez prywatnego maila, social media, gier
8. **Antywirus/antymalware** włączony i aktualizowany
9. **Regularne audyty** — kto miał dostęp do komputera, kiedy

---

6. Znane ograniczenia (uczciwie)

Chcemy być wobec Ciebie szczerzy. To są ograniczenia, nad którymi pracujemy.

`historia.db` aktualnie nie jest dodatkowo szyfrowana

Co to znaczy: Plik bazy historii pacjentów leży na Twoim dysku jako zwykły plik SQLite. Jeśli włączysz **FileVault/BitLocker** (a powinieneś), Twój dysk jest zaszyfrowany jako całość — ale **wewnątrz** Twojego konta użytkownika `historia.db` nie ma dodatkowej warstwy szyfrowania.

Praktyczne ryzyko: Jeśli ktoś już zalogował się na Twoje konto (Twoje hasło wyciekło, ktoś znał Twój PIN), zobaczy zawartość `historia.db`.

Plan naprawy: W kolejnej wersji aplikacji wprowadzamy **SQLCipher** — dodatkowe szyfrowanie samego pliku bazy danych kluczem przechowywanym w macOS Keychain / Windows Credential Manager. Wtedy nawet osoba na Twoim koncie nie odczyta `historia.db` bez Twojej zgody.

PESEL jest hashowany, ale słabo

Co to znaczy: W bazie zapisujemy PESEL w postaci „skrótu" (SHA-256 hash z prostym solem). To nie jest plaintext, ale przy znajomości struktury PESEL można odtworzyć — szczególnie dla małej praktyki.

Plan naprawy: Razem z SQLCipher wprowadzamy mocniejszy hash (PBKDF2 z indywidualną solą per pacjent) i **opcjonalnie zaszyfrowane PESELe**.

Nagrania audio czyszczone są dopiero przy końcu sesji

Co to znaczy: Surowe nagranie głosowe (`.wav`) leży na dysku przez okres pracy z badaniem — kasowane jest dopiero przy zamknięciu wizyty. Jeśli aplikacja się zawiesi przed kasowaniem, plik może zostać.

Plan naprawy: Aplikacja przy starcie skanuje folder tymczasowy i kasuje sieroce pliki audio.

---

7. Twoje prawa (RODO)

paniAnetka przetwarza Twoje dane (nie pacjentów — pacjenci są administrowani przez Ciebie) na zasadach:

- **Administrator Twoich danych:** Jan Matus, Advanced Systems Consulting and Engineering, contact@panianetka.pl (mailto:contact@panianetka.pl)
- **Cel przetwarzania:** weryfikacja licencji + faktura + (opt-in) telemetria
- **Czas przechowywania:** do końca okresu licencji + 6 lat (wymóg podatkowy dot. faktur)
- **Twoje prawa:** dostęp, sprostowanie, usunięcie, przeniesienie, ograniczenie, sprzeciw — wszystkie na adres contact@panianetka.pl (mailto:contact@panianetka.pl)

W razie usunięcia konta licencja przestaje działać — powinieneś najpierw sam wyeksportować historię pacjentów (folder `PaniAnetka/historia/`), żeby nie stracić własnych danych.

---

8. Kontakt

Pytania o ten dokument lub o sposób przetwarzania danych:

- **Email:** contact@panianetka.pl (mailto:contact@panianetka.pl)
- **Adres:** Advanced Systems Consulting and Engineering, Jan Matus
- **Strona:** panianetka.pl/dane-pacjentow (https://panianetka.pl/dane-pacjentow)

W przypadku incydentu (np. zgubiłeś laptopa z `historia.db`, zauważyłeś włamanie, zapomniałeś włączyć FileVaulta przed kradzieżą) — zalecamy:

1. Natychmiast zmień hasło użytkownika
2. Zmień hasło do każdego serwisu, do którego logowałeś się z tego komputera
3. Skontaktuj się z nami — pomożemy Ci zinwentaryzować, jakich pacjentów dotyczy incydent
4. Zgłoś **naruszenie ochrony danych** do UODO w terminie 72 h (jako administrator danych pacjentów to Twój obowiązek)

Ten dokument może się zmieniać wraz z aplikacją. Aktualna wersja zawsze dostępna na panianetka.pl/dane-pacjentow (https://panianetka.pl/dane-pacjentow) lub w aplikacji: ***Ustawienia → 🔒 Prywatność****.*

---

paniAnetka · contact@panianetka.pl · panianetka.pl