

ENG V

End-to-End Security

JEDYNE NA RYNKU PODEJŚCIE
OBEJMUJĄCE CAŁY CYKL ŻYCIA
DANYCH MEDYCZNYCH

Digitalizacja > Compliance > Cyfrowy Bunkier



IRON
MOUNTAIN®

Od fizycznego archiwum po Cyfrowy Bunkier w chmurze prywatnej

Placówki medyczne stoją dziś przed dwoma równoległymi wyzwaniami:

- rosnącą falą zaawansowanych cyberataków, które uderzają również w kopie zapasowe,
- skomplikowanymi wymogami regulacyjnymi oraz rosnącym obciążeniem administracyjnym związanym z dokumentacją.

Połączenie kompetencji Engave i Iron Mountain tworzy pełny, end2end proces bezpieczeństwa danych medycznych – od przechowywania fizycznych akt, przez digitalizację, aż po odporność cybernetyczną i odtworzenie po cyberataku.



ETAP 01

OCHRONA ARCHIWUM I ZGODNOŚĆ DOKUMENTACYJNA

Optymalizacja zarządzania dokumentacją medyczną: Od zgodności regulacyjnej po efektywność procesową.

W polskiej ochronie zdrowia kluczowe staje się jednoczesne spełnienie wymogów prawnych dotyczących archiwizacji oraz zwiększenie efektywności procesów administracyjnych. Manualne zarządzanie dokumentacją obciąża personel i ogranicza sprawność operacyjną placówki.

Iron Mountain Polska, posiadając ponad 25-letnie doświadczenie w zarządzaniu informacją, dostarcza hybrydowe rozwiązania łączące bezpieczne przechowywanie zasobów z zaawansowaną digitalizacją i automatyzacją obiegu dokumentów.

100%
compliance

100%
izolacji backupu

Natychmiastowy
dostęp do dokumentacji

Szybkie odtworzenie
systemów po ataku

FILAR I - Bezpieczeństwo fizyczne i zgodność z przepisami

DEDYKOWANA STREFA ZAMKNIĘTA

Oferujemy możliwość wydzielenia dedykowanej, zamkniętej strefy magazynowej, zaprojektowanej do przechowywania dokumentacji medycznej (w tym osobowo-płacowej) zgodnie z krajowymi wymogami.

01 ZGODNOŚĆ Z PRZEPISAMI

Nasze obiekty spełniają wymogi Rozporządzenia Ministra Kultury z 15 lutego 2005 r. oraz są regularnie i z powodzeniem kontrolowane przez Archiwum Państwowe.

02 KONTROLA DOSTĘPU

Strefy są w pełni odizolowane ścianami z materiałów niepalnych, wyposażone w systemy kontroli dostępu, a ruch osobowy jest rygorystycznie ewidencjonowany.

03 ZAAWANSOWANE BEZPIECZEŃSTWO

Gwarantujemy ochronę fizyczną 24/7, monitoring CCTV oraz zaawansowane systemy przeciwpożarowe, w tym systemy wczesnej detekcji dymu (np. VESDA).

INTEGRALNOŚĆ PROCESU LOGISTYCZNEGO

Bezpieczeństwo dokumentacji jest kluczowe również poza archiwum. Nasze procesy logistyczne są w pełni monitorowane i audytowalne (chain of custody).

01 WŁASNA FLOTA KURIERSKA

Transport realizujemy wyłącznie własną, oznakowaną flotą kurierską, wyposażoną w systemy GPS

02 PROCEDURA „CHAIN OF CUSTODY”

Każdy ruch pojemnika z dokumentacją jest wielokrotnie skanowany (minimum 6-krotnie) i rejestrowany, co zapewnia pełną kontrolę i eliminuje ryzyko zagubienia na każdym etapie – od odbioru z placówki po złożenie w lokalizacji docelowej.

Przekazanie fizycznego archiwum wyspecjalizowanemu partnerowi pozwala na optymalizację kosztów i uwolnienie cennej przestrzeni szpitalnej.



ETAP 02

DIGITALIZACJA, EKSTRAKCJA DANYCH I AUTOMATYZACJA

FILAR II: Inteligentna digitalizacja i optymalizacja pracy personelu

Prawdziwa transformacja i usprawnienie pracy personelu zaczyna się od przekształcenia dokumentów papierowych w cyfrowe. Nasze działania wpisują się w kluczowe cele Krajowego Planu Odbudowy (KPO) dla inwestycji D1.1.2, adresując zarówno Zakres 2: digitalizację dokumentacji medycznej, jak i Zakres 4: wdrożenie rozwiązań AI służących optymalizacji procesów szpitalnych oraz organizacji pracy personelu

EKSPERTYZA PROCESOWA: OD SKANU PO USTRUKTURYZOWANE DANE

Za proces digitalizacji odpowiada nasze Centrum Przetwarzania Danych w Radomiu – największy i najnowocześniejszy obiekt tego typu w Europie, wyróżniony globalnym tytułem Center of Digital Excellence.

01 SKALA I BEZPIECZEŃSTWO

Centrum działa w trybie 3-zmianowym, przetwarzając blisko 100 milionów stron rocznie. Posiada certyfikaty ISO 27001 oraz ISO 9001.

02 DOŚWIADCZENIE W PRZETWARZANIU DANYCH MEDYCZNYCH

Posiadamy bogate doświadczenie w przetwarzaniu kluczowych typów dokumentacji (realizowaliśmy ponad 150 projektów dla sektora medycznego), tj: karta informacyjna z leczenia szpitalnego, historia choroby, skierowania na badanie czy protokół operacyjny.

03 PRECYZYJNA EKSTRAKCJA DANYCH (IDP)

Nasze procesy IDP (Intelligent Document Processing) są skonfigurowane do automatycznej separacji, kategoryzacji oraz precyzyjnej ekstrakcji i indeksowania kluczowych danych, w tym:

- Rozpoznań (ICD-10)
- Procedur (ICD-9)
- Danych pacjenta (PESEL, imię, nazwisko, data urodzenia)
- Danych autora dokumentu (Imię i nazwisko, tytuł zawodowy)

JAK USPRAWNIAMY PRACĘ PERSONELU?

Automatyzujemy kluczowe czynności administracyjne, zapewniając natychmiastowy dostęp do dokumentacji, ograniczając ręczne operacje i błędy oraz przyspieszając procesy dzięki cyfrowemu obiegowi i równoległej pracy wielu użytkowników. Dzięki temu personel może skupić się na czynnościach klinicznych, a placówka zwiększa efektywność operacyjną.

PLATFORMA EVAULT® I INTEROPERACYJNOŚĆ SYSTEMÓW:

Centralne repozytorium

Zdigitalizowane dokumenty, jak i ewidencja zasobów papierowych, są dostępne poprzez bezpieczną platformę eVault®. System umożliwia autoryzowanym pracownikom placówki zarządzanie całym zasobem, wyszukiwanie oraz zamawianie oryginałów lub skanów.

Interoperacyjność (API)

Rozumiemy potrzebę integracji. Nasze rozwiązania, dzięki rozbudowanym możliwościom API, mogą płynnie łączyć się z istniejącymi w placówce systemami HIS, EDM czy PACS. Umożliwia to bezpieczną wymianę danych i włączenie zdigitalizowanych zasobów bezpośrednio w istniejące procesy szpitalne.



ETAP 03

CYFROWY BUNKIER I ODPORNOŚĆ NA RANSOMWARE

NOWA ERA CYBERATAKÓW NA SŁUŻBĘ ZDROWIA

Ataki ransomware ewoluują w zastraszającym tempie. Modele Ransomware-as-a-Service (RaaS), wspomagane przez AI, pozwalają na precyzyjne i długotrwałe ataki. Cyberprzestępcy nie ograniczają się do zaszyfrowania danych produkcyjnych – ich celem stają się również kopie zapasowe.

Dla szpitala lub jednostki medycznej, paraliż systemów HIS/PACS/RIS oznacza: Bezpośrednie zagrożenie dla zdrowia i życia pacjentów (brak dostępu do historii choroby, wyników badań, planów leczenia).

Całkowity paraliż operacyjny i gigantyczne straty finansowe.

Wysokie okupy, których zapłata nigdy nie gwarantuje odzyskania danych.

 **CYFROWY
BUNKIER™**



ROZWIĄZANIE: CYFROWY BUNKER W CHMURZE PRYWATNEJ ENGAVE

Engave oferuje unikalną usługę Cyfrowego Bunkra – w pełni zarządzanej, bezpiecznej i odizolowanej strefy do przechowywania krytycznych kopii zapasowych. To ostatnia, niezależna linia obrony, która gwarantuje odzyskanie danych nawet po najbardziej zaawansowanym ataku ransomware.

JAK DZIAŁA NASZA OCHRONA? KLUCZOWE MECHANIZMY

Budowa własnego bunkra to ogromny koszt. Engave udostępnia szpitalom zaawansowaną technologię w efektywnym kosztowo, współdzielonym modelu abonamentowym, przy wykorzystaniu zaawansowanej detekcji AI i zachowaniu pełnej logicznej separacji danych.

01 PEŁNA SUWERENNOŚĆ I BEZPIECZEŃSTWO FIZYCZNE

Dane składowane są wyłącznie na terytorium Polski w zaufanych, bezpiecznych centrach danych.

Fizyczne odmiejszczenie chroni backup przed katastrofami w głównej serwerowni (np. pożar, zalanie).

02 TECHNOLOGICZNA IZOLACJA (AIR-GAP)

Bunkier jest logicznie i sieciowo odizolowany od środowiska produkcyjnego szpitala, uniemożliwiając atakującym dostęp do kopii zapasowych.

03 NIEZMIENNOŚĆ DANYCH (IMMUTABILITY & WORM)

Kopie zapasowe są chronione mechanizmem WORM (Write Once, Read Many). Przez określony czas są absolutnie niezmiennalne – nie można ich zaszyfrować, zmodyfikować ani usunąć.

04 PROAKTYWNE SKANOWANIE

Wszystkie dane trafiające do bunkra są poddawane ciągłemu skanowaniu na obecność ransomware, złośliwego oprogramowania i śladów szyfrowania.

BEZPIECZEŃSTWO W PRZYSTĘPNYM ABONAMENCIE

KLUCZOWE KORZYŚCI

01

GWARANCJA ODTWORZENIA DANYCH

– Pewność posiadania czystej, nieskażonej kopii danych, gotowej do odtworzenia po ataku.

02

CIĄGŁOŚĆ PRACY PLACÓWKI

– Minimalizacja przestoju i szybki powrót do sprawności operacyjnej, ratujący zdrowie pacjentów.

03

ZNACZĄCA REDUKCJA KOSZTÓW

– Dostęp do technologii klasy “enterprise” (normalnie niedostępnej finansowo) w ramach przewidywalnego, miesięcznego abonamentu (OpEx zamiast CapEx).

04

PEŁNA ZGODNOŚĆ (COMPLIANCE)

– Spełnienie wymogów RODO i Ustawy o KSC dzięki lokalizacji i zabezpieczeniu danych w Polsce.

WIĘCEJ NIŻ TECHNOLOGIA – WSPARCIE EKSPERTÓW ENGAVE

DOŚWIADCZENIE POTWIERDZONE NA NAJWIĘKSZEJ INSTALACJI CYFROWEGO BUNKRA W POLSCE

Engave odpowiada za wdrożenie największego Cyfrowego Bunkra w kraju – dla Zakładu Ubezpieczeń Społecznych (ZUS), gdzie chronionych jest już ponad 1 petabajt danych. Projekt obejmuje pełną izolację, zaawansowaną detekcję ransomware i regularne testy odtworzeniowe wszystkich chronionych środowisk. To jedna z najbardziej złożonych i referencyjnych realizacji cyberodporności w Polsce.



Usługa Cyfrowego Bunkra to kompleksowe wsparcie:

Identyfikacja Środowisk Krytycznych: Pomagamy zdefiniować, które dane i systemy (oraz ich zależności) są kluczowe dla działania szpitala i muszą trafić do bunkra.

Wsparcie w Odtwarzaniu

W krytycznym momencie ataku nasi eksperci aktywnie wspierają proces odzyskiwania danych, aby jak najszybciej przywrócić działanie placówki.

Opcja: Strefa Odzyskiwania (Recovery Zone):

Możliwość rozszerzenia usługi o dedykowaną strefę (lokalną lub chmurową) do bezpiecznego uruchamiania i testowania odtwarzania systemów, gdy środowisko produkcyjne jest skompromitowane.



ETAP 04

WSPÓLNY MODEL ODPORNOŚCI DANYCH

PEŁNY CYKL ŻYCIA OCHRONY DANYCH W PLACÓWCE MEDYCZNEJ

01

BEZPIECZNE PRZEJĘCIE
I PRZECHOWYWANIE ARCHIWUM PAPIEROWEGO

02

DIGITALIZACJA, INDEKSACJA, WORKFLOW
I NATYCHMIASTOWY DOSTĘP DO DOKUMENTACJI

03

INTEGRACJA Z SYSTEMAMI HIS/PACS/RIS/EDM

04

IZOLACJA, ANALIZA
I NIEZMIENNOŚĆ KOPII ZAPASOWYCH

05

ODTWARZANIE I SZYBKI POWRÓT
DO PRACY KLINICZNEJ PO ATAKU

To jedyny na rynku model, w którym od papieru po systemy produkcyjne – cały łańcuch bezpieczeństwa jest zabezpieczony.

SKONTAKTUJ SIĘ Z NAMI, ABY WDROŻYĆ KOMPLEKSOWE
ZABEZPIECZENIE DOKUMENTACJI I SYSTEMÓW MEDYCZNYCH.



Przemysław Kędzior
Head of Sales, Engave
przemyslaw.kedzior@engave.pl
+48 662 058 624



www.engave.pl



www.ironmountain.pl