

Test odtworzenia systemu z kopii zapasowej

Kopia zapasowa, której nikt nie odtworzył, to plik na nośniku i nadzieja. Protokół prowadzi zespół przez odtworzenie jednego krytycznego systemu na osobnym serwerze, mierzy czas i utratę danych, a na koniec zostawia dokument dla dyrekcji, inspektora ochrony danych i audytora.

System objęty testem	Data testu	Kopia z dnia i godziny	Serwer odtworzenia
Cel: czas odtworzenia	Cel: utrata danych	Prowadzący test	Użytkownik weryfikujący

Czas odtworzenia liczymy od ogłoszenia awarii do chwili, gdy personel znów pracuje w systemie. Dopuszczalna utrata danych to okres pracy, którego wpisów nie ma w kopii. Oba cele bierzecie z analizy ryzyka; jeśli ich nie macie, test pokaże, jakie są naprawdę. Punkt zaznaczacie, gdy jest dowód. RODO przewiduje regularne testowanie, ale nie podaje częstotliwości; rytm ustala polityka na podstawie analizy ryzyka. Podstawa: zdolność szybkiego przywrócenia dostępności danych i regularne testowanie zabezpieczeń (art. 32 ust. 1 lit. c i d RODO), w podmiocie kluczowym lub ważnym testowanie planów ciągłości działania i odtworzenia (art. 8 ust. 1 pkt 2 lit. f ustawy o KSC), zabezpieczenie dokumentacji medycznej przed utratą i okresowa ocena skuteczności zabezpieczeń (§ 1 ust. 5 pkt 5 i ust. 7 rozporządzenia MZ o dokumentacji medycznej).

TYDZIEŃ PRZED TESTEM

Przygotowanie

- ☐ Wybraliśmy jeden system z listy krytycznych i zapisaliśmy dla niego oba cele.
Dowód: wyciąg z analizy ryzyka albo decyzja kierownika IT z datą.
- ☐ Środowisko testowe nie ma połączenia z siecią produkcyjną, platformą P1, laboratorium zewnętrznym, pocztą ani bramką SMS.
Inaczej odtworzony system drugi raz wyśle zdarzenia medyczne albo przypomnienia do pacjentów. Przy logowaniu przez domenę potrzebny jest kontroler domeny z kopii albo konta lokalne. Izolację zaleca też Centrum e-Zdrowia. Dowód: opis sieci.
- ☐ Kierownik IT i inspektor ochrony danych zgodzili się na test; wiemy, kto widzi odtworzone dane i kiedy je usuniemy.
To pełna dokumentacja medyczna: dostęp tylko dla uprawnionych, informatyk na podstawie upoważnienia administratora (art. 24 ust. 1 i ust. 2 pkt 2 ustawy o prawach pacjenta, § 1 ust. 4 pkt 1 rozporządzenia MZ o dokumentacji medycznej).
- ☐ Kopię wskazała osoba spoza zespołu, który wykonuje kopie, z miejsca odseparowanego od sieci szpitala.
Dowód: identyfikator kopii, repozytorium, data i godzina wykonania.
- ☐ Dostawca systemu potwierdził, czego od niego potrzebujemy: licencji, kluczy, instrukcji, osoby pod telefonem.
Dostawca będący podmiotem przetwarzającym ma w umowie powierzenia obowiązek pomocy przy zabezpieczeniach (art. 28 ust. 3 lit. f RODO).
- ☐ Z produkcji wzięliśmy raport na godzinę kopii: liczbę pacjentów lub dokumentów utworzonych przed kopią i numer ostatniego wpisu.
Dowód: wydruk raportu w załączniku; bez niego nie porównacie kompletności.

OD 13:00

Odtworzenie z pomiarem czasu i weryfikacja

KROK	CZYNNOŚĆ	GODZINA	KTO	UWAGI, ODSTĘPSTWA
T0	Ogłoszenie awarii, start pomiaru. Produkcji od tej chwili „nie ma”.			
1	Nośnik podłączony, hasło i klucz szyfrowania wyjęte z sejf.			
2	Serwer gotowy, system operacyjny i silnik bazy zainstalowane.			
3	Baza danych odtworzona i uruchomiona.			
4	Pliki spoza bazy odtworzone: skany, wyniki w PDF, konfiguracja.			
5	Aplikacja działa, licencja i certyfikaty przyjęte.			
6	Pierwszy użytkownik zalogowany na zwykłe konto.			

T1 Weryfikacja zakończona, koniec pomiaru.

☐ **Odtworzenie prowadziła osoba według spisanej procedury, a każde odstępstwo trafiło do uwag.**

Dowód: procedura z numerem wersji, wydrukowana albo poza odtwarzanym systemem. Jeśli zna ją tylko jedna osoba, test prowadzi ktoś inny.

☐ **Pielęgniarka, lekarz albo rejestratorka porównała z produkcją pięć losowych kart pacjentów z różnych oddziałów lub poradni.**

Porównujecie wpisy sprzed godziny kopii: wynik badania, opis obrazu, zlecenie leku, dokument podpisany elektronicznie. Dowód: pięć identyfikatorów z oceną „zgodne” lub „niezgodne”.

☐ **Raport zgadza się ze stanem zanotowanym przed testem, załączniki się otwierają, ostatni wpis ma godzinę zgodną z czasem kopii.**

Dowód: oba raporty, nazwy otwartych plików, godzina ostatniego wpisu.

POMIAR I KRYTERIA ZALICZENIA

Czas T1 minus T0 = godz. min, cel godz. W granicach celu: tak / nie.

Dane Odstęp między kopiami godz. (tyle pracy ginie przy awarii tuż przed kopią), cel godz. Tak / nie.

Zaliczony ☐ Oba cele spełnione, pięć kart zgodnych, pliki się otwierają, procedura bez improwizacji.

Warunkowo ☐ Cele spełnione, ale były odstępstwa od procedury albo braki poza danymi pacjentów.

Niezaliczony ☐ Cel przekroczony, karta niezgodna albo brak plików. Wynik trafia do kierownika podmiotu, test powtarzacie po poprawkach.

NA KONIEC DNIA

Sprzątanie, wnioski, podpisy

☐ **Środowisko testowe wyłączone, odtworzone dane pacjentów usunięte.**

Dane zostawione na serwerze testowym to ryzyko dla poufności (art. 5 ust. 1 lit. f RODO). Dowód: godzina i osoba.

☐ **Protokół z załącznikami trafił do dokumentacji bezpieczeństwa i do inspektora ochrony danych.**

W podmiocie kluczowym lub ważnym to dokumentacja operacyjna, czyli zapis poświadczający wykonanie czynności (art. 10 ust. 4 ustawy o KSC). Pozwala też wykazać przestrzeganie RODO (art. 5 ust. 2).

Co poszło inaczej niż w procedurze

Poprawki: co, kto, do kiedy

Kolejny test: system i termin

Prowadzący test

Użytkownik weryfikujący

Kierownik IT

Zatwierdził: kierownik podmiotu

Typowe błędy. Test na tym samym serwerze i w tej samej sieci sprawdza plik kopii, ale nie odtworzenie po ataku, gdy serwera już nie ma. Kopia obejmuje bazę, a skany, konfiguracja i licencja leżą poza nią. Hasło do repozytorium albo klucz szyfrowania jest tylko na serwerze, który uległ awarii. Sukces ogłasza informatyk po starcie usługi, a nikt z personelu nie otworzył karty pacjenta.

Skala ma znaczenie. Przychodnia z systemem w chmurze prosi dostawcę o odtworzenie kopii jej danych na osobnej instancji i sprawdza pięć kart; dowodem jest protokół dostawcy z godzinami, a umowa powinna taki test przewidywać. Szpital powiatowy z małym działem IT sprawdza co kwartał inny system: szpitalny, laboratoryjny, apteczny, kadrowo-płacowy. Szpital specjalistyczny z dużym archiwum obrazów odtwarza bazę systemu szpitalnego i próbkę badań z wybranych dni. Sieć placówek odtwarza centralną bazę w jednym teście, a w lokalizacjach osobno to, co przechowują u siebie. Mała przychodnia często nie podlega ustawie o KSC, ale RODO i rozporządzenie o dokumentacji medycznej obowiązują ją tak samo.

Podstawy: RODO, rozporządzenie (UE) 2016/679, art. 5 ust. 1 lit. f i ust. 2, art. 28 ust. 3 lit. f, art. 32 ust. 1 lit. c i d; ustawa z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa w brzmieniu nadanym ustawą z 23 stycznia 2026 r. (Dz.U. 2026 poz. 252), art. 8 ust. 1 pkt 2 lit. f, art. 10 ust. 4, obowiązki wdrażane do 3.04.2027 (Ministerstwo Cyfryzacji); ustawa z 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta, art. 24 ust. 1 i ust. 2 pkt 2; rozporządzenie Ministra Zdrowia z 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. 2024 poz. 798 ze zm.), § 1 ust. 4, ust. 5 pkt 5 i ust. 7; rekomendacje Centrum e-Zdrowia dotyczące kopii bezpieczeństwa (stan alarmowy CHARLIE-CRP).

Kwestia Skali, blog Arkadiusza Łobodźca o IT w ochronie zdrowia. Protokół ma charakter pomocniczy i nie zastępuje analizy prawnej ani audytu. Stan prawny na 28.09.2026. Wydawca: OneCare sp. z o.o., ul. Pokrzywy 4, 05-850 Kręcki, NIP 1182322364, KRS 0001221324. Pytania: arkadiusz.lobodziec@kwestiaskali.pl. Wersja 1.2.