Możliwość dofinansowania

Szkolenie: Bezpieczny Pacjent, Bezpieczne Dane - Cyberbezpieczeństwo i RODO w podmiotach leczniczych.

Numer usługi 2026/04/22/203083/3505527

2 300,00 PLN brutto
1 869,92 PLN netto
143,75 PLN brutto/h
116,87 PLN netto/h
196,00 PLN cena rynkowa

C4Y KATARZYNA ZASIECZNA

Brak ocen dla tego dostawcy

zdalna w czasie rzeczywistym
Usługa szkoleniowa
16 h
25.05.2026 do 26.05.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie skierowane jest do pracowników podmiotów leczniczych i ochrony zdrowia, w szczególności: • personelu rejestracji medycznej, • personelu medycznego, • pracowników administracyjnych, • kadry kierowniczej i koordynatorów, • Inspektorów Ochrony Danych / osób realizujących zadania IOD, • personelu IT oraz osób odpowiedzialnych za systemy EDM
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	24-05-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	16
Podstawa uzyskania wpisu do BUR	Znak Jakości TGLS Quality Alliance

Cel

Cel edukacyjny

Szkolenie przygotowuje uczestników do bezpiecznego przetwarzania danych osobowych i informacji medycznych w podmiotach leczniczych, w tym danych szczególnej kategorii, poprzez identyfikowanie zagrożeń cyberbezpieczeństwa,

stosowanie zasad RODO w codziennej pracy oraz prawidłowe reagowanie na incydenty bezpieczeństwa i naruszenia ochrony danych w obszarach rejestracji, działalności medycznej, administracji i IT

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje typowe zagrożenia cyberbezpieczeństwa występujące w podmiotach leczniczych (phishing, ransomware, wycieki danych, błąd ludzki)	wskazuje co najmniej 3 rodzaje zagrożeń charakterystycznych dla ochrony zdrowia	Test teoretyczny
	przypisuje zagrożenia do konkretnych obszarów pracy	Test teoretyczny
Charakteryzuje zasady przetwarzania danych osobowych w ochronie zdrowia wynikające z RODO, ze szczególnym uwzględnieniem danych szczególnej kategorii	rozróżnia dane zwykłe i dane szczególnej kategorii w kontekście medycznym	Test teoretyczny
	wskazuje właściwe podstawy przetwarzania danych pacjentów	Test teoretyczny
Identyfikuje sytuacje stanowiące naruszenie ochrony danych osobowych oraz określa obowiązki administratora danych w zakresie oceny ryzyka i terminów działań	rozpoznaje naruszenie w przedstawionym studium przypadku	Test teoretyczny
	wskazuje wymagane terminy i kierunki zgłoszeń	Test teoretyczny
Charakteryzuje role i odpowiedzialności w systemie ochrony danych (administrator danych, personel, podmiot przetwarzający, IOD)	poprawnie przypisuje zakres odpowiedzialności do poszczególnych ról	Test teoretyczny
	wskazuje konsekwencje błędnego przypisania ról	Test teoretyczny
Rozpoznaje próby wyłudzeń danych i podejmuje działania zgodnie z procedurą reagowania na incydenty	identyfikuje phishing w przykładach mail/SMS/telefon	Obserwacja w warunkach symulowanych
	wskazuje prawidłową sekwencję działań: zabezpieczenie – zgłoszenie – eskalacja	Obserwacja w warunkach symulowanych
Zbiera informacje o incydencie i uruchamia właściwe działania techniczne i organizacyjne	poprawnie uzupełnia kartę incydentu	Obserwacja w warunkach symulowanych
	wskazuje niezbędne działania zabezpieczające i naprawcze	Obserwacja w warunkach symulowanych

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Opracowuje podstawową dokumentację związaną z naruszeniem ochrony danych	przygotowuje ocenę ryzyka naruszenia	Obserwacja w warunkach symulowanych
	formułuje decyzję o zgłoszeniu oraz projekt komunikatu do osób, których dane dotyczą	Obserwacja w warunkach symulowanych
Wspiera kształtowanie kultury bezpieczeństwa informacji w zespole	komunikuje zasady bezpieczeństwa w sposób zrozumiały i adekwatny	Obserwacja w warunkach symulowanych
	proponuje działania zapobiegawcze bez eskalowania konfliktów	Obserwacja w warunkach symulowanych

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Szkolenie **„Bezpieczny Pacjent, Bezpieczne Dane – Cyberbezpieczeństwo i RODO w podmiotach leczniczych”** jest dwudniową usługą rozwojową o charakterze szkoleniowo-warsztatowym, skierowaną do pracowników podmiotów leczniczych, w szczególności personelu rejestracji medycznej, personelu medycznego, administracji, kadry kierowniczej, koordynatorów, Inspektorów Ochrony Danych oraz personelu IT.

Program szkolenia został opracowany w oparciu o obowiązujące przepisy prawa dotyczące ochrony danych osobowych, w tym RODO, oraz aktualne zagrożenia cyberbezpieczeństwa występujące w ochronie zdrowia. Zakres tematyczny szkolenia koncentruje się na bezpiecznym przetwarzaniu danych osobowych pacjentów, w tym danych szczególnej kategorii, prawidłowej organizacji pracy w obszarach rejestracji, gabinetów medycznych, administracji i systemów EDM, a także na reagowaniu na incydenty cyberbezpieczeństwa i naruszenia ochrony danych.

Szkolenie realizowane jest w formule łączącej część teoretyczną z intensywną częścią praktyczną. Wiedza przekazywana w trakcie krótkich bloków wykładowych jest każdorazowo utrwalana poprzez analizę studiów przypadków, ćwiczenia warsztatowe oraz symulacje sytuacji rzeczywistych, odzwierciedlających codzienną pracę uczestników w podmiotach leczniczych. Program umożliwia stopniowe przejście od identyfikacji zagrożeń i wymagań prawnych do samodzielnego stosowania procedur oraz podejmowania decyzji w sytuacjach incydentalnych.

Ramowy program szkolenia został opracowany w sposób zapewniający osiągnięcie wszystkich zakładanych efektów uczenia się w zakresie wiedzy, umiejętności oraz kompetencji społecznych. Treści programowe, metody dydaktyczne oraz forma zajęć są spójne z przyjętymi metodami walidacji i umożliwiają obiektywną ocenę stopnia osiągnięcia efektów uczenia się przez uczestników.

Szkolenie prowadzone jest z zachowaniem zasad dostępności, równego traktowania uczestników oraz bezpieczeństwa procesu dydaktycznego. Przerwy organizacyjne nie są wliczane do czasu trwania usługi szkoleniowej.

Program szkolenia

Dzień 1 – Cyberbezpieczeństwo w placówce medycznej

- Otwarcie, cele, test wejściowy, mapa ryzyk - Ustalenie priorytetów bezpieczeństwa w placówce; omówienie zasad pracy warsztatowej.
- Specyfika medyczna: systemy i obieg informacji (EDM/HIS, papier, wyniki) - Punkty krytyczne: rejestracja, poczekalnia, gabinet, drukarki. Checklista „czysty ekran/blat/drukarka”.
- Phishing i socjotechnika w ochronie zdrowia - Scenariusze: „rodzina pacjenta”, „NFZ/ZUS”, „laboratorium”, „serwis EDM”. Zasady weryfikacji rozmówcy.
- Warsztat 1: Rozpoznaj phishing + reakcja krok po kroku - Ćwiczenia na przykładach (mail/SMS/telefon). Gotowa checklista reakcji i eskalacji.
- Ransomware i wycieki: co robić w pierwszej godzinie - Izolacja, zgłoszenie, zabezpieczenie śladów; jakie informacje zbierać pod RODO.
- Higiena cyber w codziennej pracy - Hasła i MFA, blokada ekranu, nośniki, wydruki, praca na kontach, podstawowe zasady poufności.
- Minimum techniczne dla placówki (bez żargonu) - Kopie zapasowe, aktualizacje, dostęp zdalny, segmentacja, urządzenia medyczne – kto za co odpowiada.
- Warsztat 2: Pierwsze 60 minut incydentu - Role, decyzje, komunikacja wewnętrzna. Mini-procedura „pierwsza godzina” gotowa do wdrożenia.

Dzień 2 – RODO w ochronie zdrowia: dane szczególnej kategorii, naruszenia, prawa

- Powtórka + pytania z dnia 1 - Ustalenie obszarów do doprecyzowania, krótkie wprowadzenie do części RODO
- RODO w medycynie: dane szczególnej kategorii i podstawy przetwarzania - Art. 9: dane o zdrowiu, genetyczne, biometryczne (identyfikacja), życie seksualne. Art. 10: wyroki/naruszenia. Minimalizacja i need-to-know.
- Ochrona danych szczególnej kategorii w praktyce („w terenie”) - Rejestracja/poczekalnia/gabinet: zasady rozmowy i wywoływania. Telefon/SMS/e-mail: co wolno i jak weryfikować. Wydruki i odbiór dokumentacji. Dostępy w EDM.
- Warsztat 3: Okienko/telefon/poczekalnia – scenki i gotowe formuły - 6 scenariuszy + zestaw bezpiecznych odpowiedzi i zasad weryfikacji.
- Naruszenia ochrony danych w medycynie: ocena ryzyka, zgłoszenia, komunikaty Kiedy zgłaszać do PUODO i kiedy informować osoby. Jak opisać zakres danych medycznych bez nadmiaru. Działania naprawcze.
- Warsztat 4: Naruszenie danych medycznych - Case: błędny adresat e-maila z wynikami / zgubiony wydruk / przejęte konto. Dokumentacja, decyzja o zgłoszeniu, projekt komunikatu.
- Prawa pacjenta i innych osób: realizacja w praktyce - Dostęp i kopia danych, weryfikacja tożsamości, terminy. Sprostowanie vs dokumentacja medyczna. Ograniczenie, sprzeciw, retencja.
- Walidacja - test teoretyczny i obserwacja w warunkach symulowanych.

Walidacja

Walidacja odbywa się w formie testu teoretycznego i obserwacji w warunkach symulowanych. Kryterium zaliczenia: minimum 70% poprawnych odpowiedzi. Rozdzielność szkolenia od walidacji (rozdzielność osobowa): osoba prowadząca szkolenie nie przeprowadza końcowej walidacji. Wyniki walidacji są dokumentowane protokołem oraz arkuszem oceny/testem.

Czas trwania i organizacja

Łączny czas trwania: 16 godzin dydaktycznych (2 dni po 8 godzin). Szkolenie realizowane w godzinach zegarowych Przerwy nie są wliczone w czas trwania usługi. Liczba godzin teoretycznych: 7, liczba godzin praktycznych 8 + 1 h walidacja

Materiały dla uczestników

- ściąga: „Dane szczególnej kategorii w medycynie” (definicje + pułapki),
- checklisty: phishing, stanowisko pracy, wydruki, „pierwsza godzina incydentu”,
- szablony: karta incydentu, ocena ryzyka, rejestr wniosków/praw, matryca ról i uprawnień, szkic komunikatu do osób.

Harmonogram

Liczba przedmiotów/zajęć: 18

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 18 Dzień 1 – Cyberbezpieczeństwo w placówce medycznej - Otwarcie, cele, test wejściowy, mapa ryzyk	Jan Lis	25-05-2026	09:00	09:30	00:30
2 z 18 Specyfika medyczna: systemy i obieg informacji (EDM/HIS, papier, wyniki)	Jan Lis	25-05-2026	09:30	11:00	01:30
3 z 18 Phishing i socjotechnika w ochronie zdrowia	Jan Lis	25-05-2026	11:00	12:00	01:00
4 z 18 Warsztat 1: Rozpoznaj phishing + reakcja krok po kroku	Jan Lis	25-05-2026	12:00	13:00	01:00
5 z 18 Przerwa	Jan Lis	25-05-2026	13:00	13:30	00:30
6 z 18 Ransomware i wycieki: co robić w pierwszej godzinie	Jan Lis	25-05-2026	13:30	14:30	01:00
7 z 18 Higiena cyber w codziennej pracy	Jan Lis	25-05-2026	14:30	15:30	01:00
8 z 18 Warsztat 2: Pierwsze 60 minut incydentu	Jan Lis	25-05-2026	15:30	16:30	01:00
9 z 18 Minimum techniczne dla placówki (bez żargonu)	Jan Lis	25-05-2026	16:30	17:30	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
10 z 18 Dzień 2 – RODO w ochronie zdrowia: dane szczególnej kategorii, naruszenia, prawa. Powtórka + pytania z dnia 1	Jan Lis	26-05-2026	09:00	09:30	00:30
11 z 18 RODO w medycynie: dane szczególnej kategorii i podstawy przetwarzania	Jan Lis	26-05-2026	09:30	10:30	01:00
12 z 18 Ochrona danych szczególnej kategorii w praktyce („w terenie”)	Jan Lis	26-05-2026	10:30	12:00	01:30
13 z 18 Warsztat 3: Okienko/telefon/ poczekalnia – scenki i gotowe formuły	Jan Lis	26-05-2026	12:00	13:00	01:00
14 z 18 Przerwa	Jan Lis	26-05-2026	13:00	13:30	00:30
15 z 18 Naruszenia ochrony danych w medycynie: ocena ryzyka, zgłoszenia, komunikaty	Jan Lis	26-05-2026	13:30	14:30	01:00
16 z 18 Warsztat 4: Naruszenie danych medycznych	Jan Lis	26-05-2026	14:30	15:30	01:00
17 z 18 Prawa pacjenta i innych osób: realizacja w praktyce	Jan Lis	26-05-2026	15:30	16:30	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
18 z 18 Walidacja - tekst teoretyczny i obserwacja w warunkach symulowanych	-	26-05-2026	16:30	17:30	01:00

Cennik

Jeżeli korzystasz z dofinansowania w wysokości co najmniej 70% przysługuje Tobie zwolnienie z podatku VAT

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 300,00 PLN
Koszt przypadający na 1 uczestnika netto	1 869,92 PLN
Koszt osobogodziny brutto	143,75 PLN
Koszt osobogodziny netto	116,87 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Jan Lis

Manager IT, administrator sieci oraz kierownik działu IT z ponad 20-letnim doświadczeniem zawodowym w sektorze technologicznym. Obecnie pełni funkcję Kierownika IT w Szpitalu Wojewódzkim w Poznaniu, wcześniej Kierownika Działu Informatyki w Specjalistycznym Zespole Opieki Zdrowotnej nad Matką i Dzieckiem w Poznaniu.
Odpowiadał za utrzymanie ciągłości działania systemów szpitalnych, nadzór nad infrastrukturą sieciową oraz bezpieczeństwo baz danych i systemów medycznych. Jego kluczowym osiągnięciem było wdrożenie pełnej infrastruktury IT Wielkopolskiego Centrum Pediatrii.

Doświadczenie w zakresie szkoleń i weryfikacji umiejętności

Posiada doświadczenie w realizacji szkoleń w obszarze IT, cyberbezpieczeństwa oraz bezpieczeństwa informacji w podmiotach publicznych i medycznych, zdobyte w ciągu ostatnich pięciu lat. Prowadził szkolenia i działania edukacyjne dotyczące ochrony danych, bezpieczeństwa systemów, zarządzania incydentami oraz wdrażania procedur IT zgodnych z wymaganiami

prawnymi i normatywnymi.
Weryfikuje efekty uczenia się uczestników poprzez zadania praktyczne, analizę przypadków oraz ocenę stosowania procedur bezpieczeństwa.

Wykształcenie i kwalifikacje

Absolwent Uniwersytetu im. Adama Mickiewicza w Poznaniu (fizyka). Ukończył studia podyplomowe z zakresu zarządzania projektami IT, administrowania bezpieczeństwem informacji oraz cyberbezpieczeństwa w sektorze publicznym. Certyfikowany Audytor Wewnętrzny ISO/IEC 27001:2013.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały dla uczestników

- ściąga: „Dane szczególnej kategorii w medycynie" (definicje + pułapki),
- checklisty: phishing, stanowisko pracy, wydruki, „pierwsza godzina incydentu",
- szablony: karta incydentu, ocena ryzyka, rejestr wniosków/praw, matryca ról i uprawnień, szkic komunikatu do osób.

Informacje dodatkowe

- Warunkiem uzyskania zaświadczenia jest uczestnictwo w co najmniej 80% zajęć usługi rozwojowej
- 1 godzina rozliczeniowa = 60 minut
- przerwy nie wliczają się do czasu szkolenia
- Karta niniejszej usługi rozwojowej została przygotowana zgodnie z obowiązującym Regulaminem Bazy Usług Rozwojowych

Zapisując się na usługę wyrażasz zgodę na rejestrowanie/nagrywanie swojego wizerunku na potrzeby monitoringu, kontroli oraz w celu utrwalenia efektów uczenia się.

Usługa może być zwolniona z VAT dla Uczestników, których poziom dofinansowania wynosi co najmniej 70% na podstawie § 3 ust. 1 pkt. 14 Rozporządzenia Ministrów Finansów z 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień.

Warunki techniczne

Platforma: MS Teams

iOS: iOS 11

Windows: Windows 10 kompilacja 14393

Android: Android OS 5.0

Funkcje sieci Web. Najnowsza wersja przeglądarki Safari, Internet Explorer 11, Chrome, Edge lub Firefox

Komputer Mac: MacOS 10.13

Połączenie internetowe: wymagane jest połączenie internetowe przewodowe lub bezprzewodowe (3G, 4G, LTE) o następujących parametrach:

- dla transmisji wideo w jakości HD 720p minimalna przepustowość łącza internetowego wynosi: 1.5Mbps/1.5Mbps (wysyłanie/odbieranie).

- dla transmisji wideo w jakości FullHD 1080p minimalna przepustowość łącza internetowego wynosi: 3Mbps/3Mbps (wysyłanie/odbieranie).

Okres ważności linku: Link będzie ważny w dniach i godzinach wskazanych w harmonogramie usługi.

Link: będzie udostępniony i umieszczony w karcie na 5 dni roboczych przed szkoleniem.

Kontakt

KATARZYNA ZASIECZNA

E-mail katarzynazasieczna@gmail.com

Telefon (+48) 668 163 580