Możliwość dofinansowania

C4Y KATARZYNA ZASIECZNA

Brak ocen dla tego dostawcy

Szkolenie: Bezpieczna dokumentacja medyczna oraz pozostała dokumentacja związana z funkcjonowaniem placówki i cyberbezpieczeństwo w szpitalu

Numer usługi 2026/04/12/203083/3480693

836,40 PLN brutto
680,00 PLN netto
52,28 PLN brutto/h
42,50 PLN netto/h
261,33 PLN cena rynkowa

Piekary Śląskie
Usługa szkoleniowa
stacjonarna
16:00 h
10.10.2026 do 10.10.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Usługa skierowana jest do pracowników podmiotów leczniczych i ochrony zdrowia, w szczególności do: personelu rejestracji medycznej, personelu medycznego, pracowników administracyjnych, kadry kierowniczej i koordynatorów, osób odpowiedzialnych za obieg i przechowywanie dokumentacji medycznej oraz pozostałej dokumentacji związanej z funkcjonowaniem placówki, a także pracowników wspierających obsługę systemów informatycznych. Warunki uczestnictwa: podstawowa umiejętność obsługi komputera i poczty elektronicznej oraz wykonywanie zadań związanych z pracą na dokumentacji lub informacjach przetwarzanych w placówce
Minimalna liczba uczestników	15
Maksymalna liczba uczestników	35
Data zakończenia rekrutacji	09-10-2026
Forma prowadzenia usługi	stacjonarna
Liczba godzin usługi	16
Podstawa uzyskania wpisu do BUR	Znak Jakości TGLS Quality Alliance

Cel

Cel edukacyjny

Szkolenie przygotowuje uczestników do bezpiecznej pracy z dokumentacją medyczną oraz pozostałą dokumentacją związaną z funkcjonowaniem placówki, zarówno w postaci elektronicznej, jak i papierowej, poprzez rozwinięcie praktycznych kompetencji w zakresie ochrony danych osobowych, poufności informacji o pacjencie, bezpiecznych nawyków pracy oraz prawidłowego reagowania na incydenty bezpieczeństwa i naruszenia ochrony danych w warunkach szpitalnych.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozróżnia rodzaje dokumentacji i informacji przetwarzanych w szpitalu oraz identyfikuje ryzyka ich ujawnienia.	przyporządkowuje wskazane przykłady do właściwych kategorii dokumentacji (medyczna / niemedyczna)	Test teoretyczny
	identyfikuje co najmniej 3 zagrożenia dla poufności lub dostępności informacji na podstawie opisanych sytuacji.	Test teoretyczny
Stosuje zasady bezpiecznej pracy z dokumentacją elektroniczną i papierową.	wskazuje prawidłowe zasady logowania i zabezpieczania dostępu do systemów oraz dokumentów	Test teoretyczny
	wybiera prawidłowe postępowanie w opisanych sytuacjach dotyczących obiegu, przechowywania i archiwizacji dokumentów.	Test teoretyczny
Wyjaśnia zasady poufności w komunikacji z pacjentem oraz osobami uprawnionymi.	wskazuje prawidłowe sposoby weryfikacji tożsamości pacjenta lub osoby uprawnionej,	Test teoretyczny
	rozróżnia sytuacje, w których można udzielić informacji od sytuacji wymagających odmowy	Test teoretyczny
Rozpoznaje podstawowe zagrożenia cyberbezpieczeństwa w szpitalu	rozpoznaje co najmniej 3 rodzaje zagrożeń (np. phishing, ransomware, błędny adresat),	Test teoretyczny
	identyfikuje symptomy incydentu bezpieczeństwa na podstawie opisu sytuacji	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Podejmuje prawidłowe pierwsze działania po stwierdzeniu incydentu lub naruszenia danych.	wskazuje prawidłową kolejność działań po incydencie (zabezpieczenie, zgłoszenie, ograniczenie skutków)	Test teoretyczny
	wybiera poprawne postępowanie w opisanych scenariuszach incydentowych.	Test teoretyczny

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 przygotowuje do bezpiecznego i zgodnego z obowiązującymi zasadami przetwarzania informacji oraz dokumentacji w podmiocie leczniczym, ze szczególnym uwzględnieniem środowiska pracy, w którym równolegle wykorzystywana jest dokumentacja elektroniczna oraz papierowa. Uczestnicy rozwijają umiejętności identyfikowania zagrożeń dla poufności, integralności i dostępności danych oraz stosowania właściwych zasad postępowania w codziennych sytuacjach zawodowych.

Program szkolenia koncentruje się na praktycznych aspektach pracy w szpitalu i odnosi się do rzeczywistych zdarzeń oraz błędów, które najczęściej prowadzą do incydentów bezpieczeństwa informacji. Uczestnicy analizują przykłady sytuacyjne, rozpoznają ryzyka oraz dobierają właściwe działania zapobiegawcze i korygujące, możliwe do wdrożenia w miejscu pracy bezpośrednio po zakończeniu szkolenia.

Warunki organizacyjne

Usługa realizowana jest w sali szkoleniowej, wyposażonej w stanowiska dla uczestników oraz trenera, umożliwiającej prowadzenie zajęć w formie wykładowo-warsztatowej. Sala posiada dostęp do energii elektrycznej oraz sprzęt multimedialny umożliwiający wyświetlanie prezentacji (np. rzutnik lub ekran). Układ sali zapewnia warunki do realizacji ćwiczeń sytuacyjnych oraz przeprowadzenia walidacji w formie testu teoretycznego.

Szkolenie prowadzone jest z zachowaniem zasad dostępności, równego traktowania uczestników oraz bezpieczeństwa procesu dydaktycznego.

Metody dydaktyczne: wykład na żywo, omówienie zagadnień praktycznych, analiza przypadków z pracy podmiotu leczniczego, ćwiczenia sytuacyjne i warsztatowe, dyskusja moderowana oraz rekomendacje wdrożeniowe.

Walidacja: walidacja odbywa się w formie testu teoretycznego obejmującego pytania problemowe i scenariuszowe; sprawdzające osiągnięcie efektów uczenia się. Kryterium zaliczenia: minimum 70% poprawnych odpowiedzi.

Rozdzielność szkolenia od walidacji: osoba prowadząca szkolenie nie przeprowadza końcowej walidacji. Wyniki walidacji są dokumentowane protokołem oraz arkuszem testowym.

Warunek uzyskania dokumentu potwierdzającego ukończenie usługi: Uczestnictwo w co najmniej 80% zajęć oraz pozytywny wynik walidacji.

Program szkolenia

- Moduł 1. Dokumentacja elektroniczna: bezpieczna praca z EDM/HIS i innymi systemami wykorzystywanymi w szpitalu, logowanie, dostępy, odpowiedzialność za konta, widoczność danych na ekranie, współdzielone stanowiska pracy.
- Moduł 2. Dokumentacja papierowa: przechowywanie, obieg, wydruki, kopiowanie, transport dokumentacji i archiwizacja zgodnie z zasadą clean desk, clean screen i bezpieczna drukarka.
- Moduł 3. Poufność informacji o pacjencie: rozmowy w rejestracji, na oddziale, w gabinecie i przez telefon; weryfikacja tożsamości; przekazywanie informacji pacjentowi i osobom uprawnionym.
- Moduł 4. Cyberbezpieczeństwo w szpitalu: phishing, fałszywe e-maile, SMS-y i połączenia, przejęcie kont, ransomware, nośniki danych, blokada ekranu, bezpieczne nawyki użytkownika.
- Moduł 5. Incydenty i naruszenia: rozpoznawanie incydentu bezpieczeństwa lub naruszenia ochrony danych; pierwsze działania po stwierdzeniu zdarzenia; ograniczanie skutków.
- Warsztat praktyczny: analiza sytuacji występujących w pracy szpitala, rozpoznawanie zagrożeń i dobre praktyki reakcji; wskazanie działań poprawy możliwych do wdrożenia bezpośrednio po szkoleniu.
- Walidacja - test teoretyczy

Czas trwania i organizacja

Łączny czas trwania: 9 godzin dydaktycznych. Szkolenie realizowane w godzinach zegarowych Przerwy nie są wliczone w czas trwania usługi. Liczba godzin teoretycznych: 5, liczba godzin praktycznych 3 + 1 h walidacja

Harmonogram

Liczba pozycji harmonogramu: 12

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 12 Otwarcie szkolenia, cele usługi, omówienie zasad pracy i mapy ryzyk.	Jan Lis	10-10-2026	08:00	08:15	00:15
2 z 12 Moduł 1. Dokumentacja elektroniczna – bezpieczna praca z systemami i kontami.	Jan Lis	10-10-2026	08:15	09:30	01:15
3 z 12 Przerwa	Jan Lis	10-10-2026	09:30	09:45	00:15

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
4 z 12 Moduł 2. Dokumentacja papierowa – obieg, wydruki, archiwizacja, clean desk / clean screen.	Jan Lis	10-10-2026	09:45	10:45	01:00
5 z 12 Przerwa	Jan Lis	10-10-2026	10:45	11:00	00:15
6 z 12 Moduł 3. Poufność informacji o pacjencie – rozmowy, telefon, weryfikacja tożsamości.	Jan Lis	10-10-2026	11:00	12:00	01:00
7 z 12 Przerwa	Jan Lis	10-10-2026	12:00	12:30	00:30
8 z 12 Moduł 4. Cyberbezpieczeń stwo w szpitalu – phishing, ransomware, hasła, nośniki, nawyki użytkownika.	Jan Lis	10-10-2026	12:30	13:30	01:00
9 z 12 Przerwa	Jan Lis	10-10-2026	13:30	13:45	00:15
10 z 12 Moduł 5. Incydenty i naruszenia – pierwsze działania, zgłoszenie, ograniczanie skutków.	Jan Lis	10-10-2026	13:45	14:45	01:00
11 z 12 Warsztat praktyczny i rekomendacje wdrożeniowe.	Jan Lis	10-10-2026	14:45	15:15	00:30
12 z 12 Walidacja - test teoretyczny	-	10-10-2026	15:15	16:00	00:45

Cennik

Jeżeli korzystasz z dofinansowania w wysokości co najmniej 70%, możesz mieć możliwość skorzystania ze zwolnienia z podatku VAT, pod warunkiem spełnienia pozostałych wymogów, o których mowa w § 3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	836,40 PLN
Koszt przypadający na 1 uczestnika netto	680,00 PLN
Koszt osobogodziny brutto	52,28 PLN
Koszt osobogodziny netto	42,50 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 szkoleniowe w formie elektronicznej lub drukowanej, zestaw dobrych praktyk oraz rekomendacje wdrożeniowe.

Informacje dodatkowe

- Warunkiem uzyskania zaświadczenia jest uczestnictwo w co najmniej 80% zajęć usługi rozwojowej
- 1 godzina rozliczeniowa = 45minut
- 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.

Adres

ul. Bytomska 62
41-940 Piekary Śląskie
woj. śląskie

Udogodnienia w miejscu realizacji usługi

- Wi-fi

Kontakt

KATARZYNA ZASIECZNA

E-mail katarzynazasieczna@gmail.com
Telefon (+48) 668 163 580