OCHRONA DANYCH OSOBOWYCH W SŁUŻBIE ZDROWIA

NOWE WYZWANIA PLACÓWEK LECZNICZYCH JAKO ADMI ISTRATORÓW DANYCH

Wokół zmieniających się przepisów w zakresie ochrony danych osobowych, zarówno w prawie polskim, jak i europejskim, narasta wiele mitów i nadinterpretacji. Nie łatwo też nadążyć za zmianami w przepisach dotyczących służby zdrowia, zwłaszcza dotyczących elektronicznej dokumentacji medycznej. W placówkach leczniczych zasady i procedury ochrony danych osobowych muszą mieć przecież bardzo ważną rangę. Warto w tym wszystkim wiedzieć na co w pierwszej kolejności zwrócić uwagę, co jest ważne, a co ważniejsze, jak się odpowiednio przygotować na nadchodzące zmiany i jak zadbać o aktualny stan ochrony danych zgodny z obowiązującymi przepisami. Zapraszamy na praktyczne w tym względzie szkolenie. Uczestnicy dotychczasowych szkoleń na ten temat wystawiali prowadzącemu najwyższe oceny za merytoryczną i praktyczną wartość oraz poziom przydatności przekazywanej wiedzy. W ciekawy sposób prezentowane są formalne i praktyczne aspekty ochrony danych osobowych w służbie zdrowia.

CEL

Omówienie najnowszych zmian w ustawie o ochronie danych osobowych oraz ustawie o prawach pacjenta i Rzeczniku praw pacjenta.. Przygotowanie do stosowania zmienionych przepisów o ochronie danych osobowych.

Omówienie nowych obowiązków i roli administratora bezpieczeństwa informacji. Omówienie wszelkich aspektów wykonywania funkcji ABI po 1 stycznia 2015 r. Analiza wyboru pomiędzy powołaniem ABI, a wyznaczeniem wewnętrznego specjalisty ds. ochrony danych – dopóki jest taki wybór, zwłaszcza dla placówek ochrony zdrowia.

Omówienie technicznych i organizacyjnych wymogów względem elektronicznej dokumentacji medycznej i danych osobowych. Umiejętność zastosowania w praktyce zasad przetwarzania danych oraz wymaganych organizacyjnych i technicznych środków bezpieczeństwa stosowanych do ich ochrony.

Analiza paragrafu 20 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

ADRESACI WARSZTATÓW

Warsztaty kierowane są do administratorów danych (tj. właścicieli, dyrektorów, prezesów placówek), administratorów bezpieczeństwa informacji i osób przygotowywanych do pełnienia takiej roli,

administratorów systemów informatycznych - Informatyków, kadry zarządzającej odpowiedzialnej za bezpieczeństwo danych w podmiotach leczniczych, w tym za dane personalne, menedżerów, dyrektorów, kierowników działów IT/administracji w podmiotach leczniczych, pracowników administracji samodzielnych publicznych zakładów opieki zdrowotnej, właścicieli praktyk zawodowych.

TREŚCI PROGRAMOWE

1. Omówienie najważniejszych zmian w przepisach prawa, zarówno krajowych, jak i europejskich, z zakresu ochrony danych osobowych i danych medycznych.
2. Podstawy prawne wyznaczenia ABI w placówce medycznej, zakres jego praw i obowiązków oraz umiejscowienie w strukturze organizacji.
3. Ustawowe obowiązki Administratora danych i rola ABI w praktycznym nadzorze nad ich realizacją i przestrzeganiem, zarówno w wariancie zgłoszenia ABI do GIODO, jak i bez takiego zgłoszenia.
4. Co wynika z możliwości zarejestrowania ABI u GIODO, zwłaszcza w zakresie rejestracji zbiorów danych i uprawnień kontrolnych. Korzyści, a obowiązki. Czy powołanie ABI to opcja, czy obowiązek i jak długo będzie taki wybór.
5. Prawne oraz organizacyjne aspekty powierzenia przetwarzania danych osobowych, w tym możliwość korzystania z usług specjalistów zewnętrznych, jako ABI i ASI (administratora systemu informatycznego).
6. Obowiązki ADO, ABI, ASI i wyjaśnienie dlaczego powołanie administratora systemów informatycznych nie koniecznie jest dobrym pomysłem.
7. Praktyczne omówienie obowiązków i środków bezpieczeństwa wymaganych ustawą o ochronie danych osobowych, ustawą o systemie informacji w ochronie zdrowia, Rozporządzeniem „KRI", a w szczególności:

a) zasady przechowywania danych przetwarzanych w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych,

b) mechanizmy kontroli dostępu do danych przetwarzanych w systemach informatycznych

c) stosowane zabezpieczenia przed zagrożeniami pochodzącymi z sieci publicznej

d) funkcjonalności stosowane w systemach informatycznych w zakresie realizacji wymogów wynikających z przepisów o ochronie danych osobowych

8. Co powinny zawierać dokumenty Polityki bezpieczeństwa informacji, Instrukcji zarządzania systemem informatycznym, jakie załączniki, instrukcje, regulaminy powinny je uzupełniać.
9. Zasady przetwarzania danych osobowych i danych medycznych. Kiedy i jaka klauzula informacyjna, a kiedy klauzula zgody.
10. Możliwości i zasady korzystania z usług chmur obliczeniowych (Cloud Computing), zwłaszcza w Zakładach Opieki Zdrowotnej.
11. Skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna.
12. Przykłady wykradania danych, największych „wycieków". Metody przeciwdziałania.

METODY I NARZĘDZIA DYDAKTYCZNE

Szkolenie prowadzone w konwencji warsztatowej, z możliwością zadawania pytań w trakcie wykładów. Omawiane będą praktyczne przykłady i codzienne sytuacje oraz dotychczasowe decyzje GIODO i wyroki NSA. Uczestnicy spotkania będą mogli otrzymać odpowiedzi i informacje na problemy dotyczące wykonywania zadań w ich konkretnych Organizacjach, a jednocześnie wymienić się swoimi

doświadczeniami i spostrzeżeniami z innymi uczestnikami. Uczestnicy otrzymają materiały szkoleniowe wraz z pomocnymi wzorami różnych instrukcji, regulaminów i harmonogramów kontroli w formie papierowej i elektronicznej. Gwarancję skuteczność i przydatności informacji i materiałów zapewnia wiedza i wieloletnia praktyka prowadzącego szkolenie. Poznają Państwo najważniejsze zadania i największe problemy związane z wykonywaniem obowiązków administratora bezpieczeństwa informacji jednocześnie poznając sposoby realizacji obowiązków i możliwości rozwiązywania potencjalnych problemów.

PRELEGENT:

Piotr Glen – Specjalista ds. ochrony danych osobowych. Praktyk, mający wieloletnie doświadczenie w stosowaniu prawa ochrony danych osobowych oraz wdrażaniu polityki bezpieczeństwa informacji w setkach różnego rodzaju instytucjach, również w placówkach ochrony zdrowia. Członek Stowarzyszenia Administratorów Bezpieczeństwa Informacji SABI i jako uczestniczył w konsultacjach nad rozporządzeniami wykonawczymi do zmienionej ustawy o ochronie danych osobowych. Doświadczony Administrator Bezpieczeństwa Informacji pełniący tę funkcję dla wielu firm i instytucji. Audytor Systemu Zarządzania Bezpieczeństwem Informacji wg PN-ISO/IEC 27001 (Certyfikat Polskiego Komitetu Normalizacyjnego Nr 28/SZBI/2013). Autor wielu publikacji w zakresie ochrony danych osobowych (min w Serwisie Kadry Zarządzającej ZOZ www.serwiszoz.pl , Magazynie Menadżerów Ochrony Zdrowia www.healthcare.wip.pl , kwartalniku „Nowe technologie IT w ochronie zdrowia”). Trener, prelegent, wykładowca akademicki. Uczestnik, jako ABI, postępowań administracyjnych oraz kontroli prowadzonych przez GIODO. Posiada duże doświadczenie i bardzo dobre umiejętności w prowadzeniu szkoleń z praktycznych aspektów ochrony danych osobowych. Dysponując źródłową wiedzą w rzetelny, praktyczny i uczciwy sposób przedstawia jak osiągnąć stan ochrony danych zgodny z aktualnymi przepisami prawa.