mgr Adam Piątek

Bezpieczeństwo Informacji prawnie chronionych w jednostkach świadczących usługi medyczne.

Legally protected information security in medical facilities.

mgr Adam Piątek
Specjalista d/s Informacji Prawnie Chronionych i Bezpieczeństwa Informacji w Standarder Sp. z o.o.,
www.standarder.pl

Podczas wizyty w zaprzyjaźnionym prywatnym gabinecie lekarskim zainteresowałem się oprogramowaniem, jakiego używa się do bieżącej obsługi pacjentów. Podkreślono, że jest to jeden z bardziej zinformatyzowanych gabinetów tego typu. „Mamy tu wszystkie dane pacjentów, historie choroby, wystawione recepty…" Kontynuując temat, zapytałem o bezpieczeństwo tych danych. „Oczywiście dane są zabezpieczone, do programu trzeba się zalogować. Może Pan sprawdzić". Nie wnikając w fakt, że w ogóle nie powinienem mieć możliwości dostania się do komputera, złamanie hasła dostępu zajęło mi niecałe pięć minut (sic!).

Na pytanie, co by stało gdyby dane pacjentów zawarte w programie zostały upublicznione - nawet nieumyślnie- we wszechobecnym Internecie, nie uzyskałem odpowiedzi. Jak sądzę, wizja była zbyt przerażająca.

Ten skrajny być może przykład pozwala uzmysłowić sobie, jaką wartość mają informacje przetwarzane w naszych jednostkach. Punktem wyjścia do analizy tematu jest zawsze ocena z jakimi informacjami mamy do czynienia w naszych placówkach.

Jako kryterium klasyfikacji stosując przepisy prawa w Polsce, informacje możemy podzielić na informacje publiczne, informacje bezwzględnie chronione przepisami prawa oraz informacje chronione względnie, dla których przepisy prawa umożliwiają ochronę.

Streszczenie

Wartość informacji w dzisiejszym biznesie jest coraz bardziej znacząca. Utrata, upublicznienie tajemnic handlowych lub informacji prawnie chronionych firmy może prowadzić do strat finansowych lub nawet jej upadku. W artykule przedstawiono podstawowe zagadnienia dotyczące informacji prawnie chronionych w placówkach medycznych.

Abstract

Nowadays, the value of information in business is becoming more and more significant. Loss, publication of trade secrets or legally protected information may cause financial losses in the company or even its downfall. This article presents the basic concept of legally protected information in medical facilities.

Informacje publiczne

Pierwszą grupą informacji o naszych firmach są informacje publicznie dostępne. Możemy tutaj wymienić wszelkie informacje dostępne w publicznych rejestrach, takich jak KRS albo KRD do umieszczania których obligują nas przepisy prawa; także informacje na różnego rodzaju portalach informacyjnych branżowych, geolokalizacyjnych, forach internetowych lub na portalach społecznościowych czy naszych stronach internetowych. Ze względu na publiczność tych informacji, ich kontrola jest trudna, co jednak nie znaczy, że należy je lekceważyć. Niekoniecznie prawdziwa opinia o naszych usługach lub niefortunne zdjęcie z wyjazdu integracyjnego umieszczone na portalu społecznościowym może przynieść nam sporo strat finansowych. Taką grupę informacji należy nieustannie monitorować lub zlecić specjalistycznej agencji zajmującej się takim monitoringiem. Do informacji publicznych należą również informacje biznesowe, celowo podawane przez nas samych do wiadomości publicznej dla kreowania naszego wizerunku. Są to informacje o kwalifikacjach pracowników, nowych metodach leczenia czyli produktach; nformacje zachęcające potencjalnych klientów do skorzystania z naszych usług.

Informacje prawnie chronione bezwzględnie

Druga grupa informacji to informacje prawnie chronione bezwzględnie. Nie mamy tutaj możliwości niestosowania przepisów prawa. Są to informacje, za których nieprawidłowe przetwarzanie grożą sankcje prawne. Do tej grupy informacji należą min. informacje niejawne podlegające ustawie o informacjach niejawnych oraz dane osobowe. Ze względu na ich powszechność, skoncentrujmy się na danych osobowych.

W związku z rosnącą świadomością prawa ochrony prywatności, wzrasta ilość roszczeń osób prywatnych o naruszenie ich prawa do prywatności. Coraz częściej prawo to zostaje wykorzystywane przy okazji innej sytuacji spornej. Obecnie w całej Unii Europejskietrwają przygotowania nowelizacji prawa ochrony danych osobowych, co prawdopodobnie spowoduje nasilenie takich działań. Niekontrolowany, nawet nieumyślny wyciek danych osobowych i ich bezprawne udostępnienie może skutkować dla nas konsekwencjami prawnymi, finansowymi, kontrolami utrudniającymi działalność oraz pogorszeniem wizerunku.

W przypadku placówek służby zdrowia mamy do czynienia z danymi osobowymi w zakresu tzw. danych wrażliwych. Dopuszczalność i zakres przetwarzania tych danych (dane medyczne) regulują ustawy branżowe (min. ustawa z 30 sierpnia 1991 roku o zakładach opieki zdrowotnej, Ustawa z 6 listopada 2008 roku o prawach pacjenta i rzeczniku praw pacjenta, rozporządzenie Ministra Zdrowia zmieniające rozporządzenie w sprawie rodzajów i zakresu dokumentacji medycznej w zakładach opieki zdrowotnej oraz sposobu jej przetwarzania) oraz (ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. wraz z obowiązującym rozporządzeniem z dnia 29 kwietnia 2004 r.w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych). Do danych osobowych zaliczamy wszelkie informacje dotyczące osoby, a więc nie tylko dane teleadresowe czy dokumentację medyczną, ale wszelkie inne informacje o pacjencie, do których dostęp mają np. pracownicy. Te informacje również podlegają ochronie prawnej.

Temat ochrony danych osobowych jest jednym z trudniejszych do „ogarnięcia" w jednostce ze względu na to, że osoba odpowiedzialna za ten obszar działalności powinna posiadać zarówno kompetencje informatyczne, jak i kwalifikacje z dziedziny prawa. Skrajnym przypadkiem jest pozostawienie odpowiedzialności na barkach właściciela lub prezesa, nieświadomego zagrożeń nieuprawnionego dostępu do danych, oraz odpowiedzialności prawnej.

Problemy organizacji systemu ochrony danych osobowych.

Obecnie obowiązujące przepisy ustawy o ochronie danych osobowych definiują zasady ich przetwarzania oraz minimalne wymagania dotyczące warunków technicznych i organizacyjnych koniecznych do spełnienia w procesie przetwarzania. Celem wyjaśnienia, jako przetwarzanie rozumie się jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie danych. Wszelkie te czynności muszą podlegać restrykcyjnym zasadom gwarantującym ich poufność, integralność i rozliczalność. Podstawowe wymagania wynikające z rozporządzenia do ustawy to wdrożenie polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym. Wdrożona dokumentacja musi zawierać szereg elementów opisujących sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę ich przetwarzanych.

Najczęstszymi błędami popełnianymi w polityce bezpieczeństwa oraz przetwarzaniu danych osobowych w podmiotach medycznych są:

- niewłasciwe definicje zbiorów danych osobowych i przepływów pomiędzy systemami lub ich brak
- zbyt szeroki zakres danych nie wynikający bezpośrednio z ustaw branżowych bez wymaganej zgody pacjenta
- brak rejestracji zbiorów w GIODO (Generalny Inspektor Ochrony Danych Osobowych) - poza danymi pacjentów z zasady nie wymagającymi rejestracji tworzone są inne zbiory danych jak subskrybenci newsletterów, uczestnicy programów lojalnosciowych, dane pacjentów wykorzystywane w celach marketingowych
- nieznajomość procedur zawartych w polityce i przepisów ochrony danych przez personel
- brak upoważnień dla personelu do przetwarzania danych lub niewłaściwe nadanie zakresów
- brak wyznaczonej osoby odpowiedzialnej za zagadnienia ochrony danych osobowych (administartor bezpieczeństwa informacji)
- brak udokumentowanych podstaw prawnych przetwarzania danych osobowych
- brak udokumentowanych podstaw prawnych udostępniania lub przekazywania danych
- utożsamianie zwolnienienia z rejestracji zbiorów danych medycznych ze zwonieniem z ustawy o ochronie danych osobowych.

Do najczęściej popełnianych błędów z zakresu zarządzania systemem informatycznym należą:

- nieokreślenie zakresów odpowiedzialności
- brak kontroli zewnętrznej nad prawidłowym przetwarzaniem danych w systemach informatycznych
- nieprawidłowy system zarządzania dostępem do systemów informatycznych
- brak integralności danych w dokumentacji elektronicznej i dokumentacji papierowej
- brak nadzoru nad niekontrolowanym przekazywaniem danych przez personel np. pocztą elektroniczną,
- niezapewnienie obowiązku rozliczności danych osobowych
- wdrażanie nowych rozwiązań bez konsultacji z zakresu bezpieczeństwa i ochrony prywatności
- nieprawidłowości w infrastrukturze technicznej
- niekompletna klasyfikacja urządzeń przetwarzających danych (np. urządzenia radiologiczne przechowują dane osobowe)
- nieświadomy personel, (brak szkoleń)

Prawidłowe zajęcie się tematem ochrony danych osobowych jest procesem korzystnym dla całej jednostki, wymusza uporządkowanie większości obiegu informacji w jednostce, wzmacnia bezpieczeństwo, eliminując zagrożenia i porządkuje obieg informacji w szerokim zakresie. W prawidłowym uporządkowaniu warto skorzystać ze specjalistycznej bezstronnej pomocy potrafiącej kompetentnie ocenić niuanse zarówno prawne, jak i strukturę informatyczną.

Informacje prawnie chronione względnie

Informacje chronione ustawą o zwalczaniu nieuczciwej konkurencji z dnia 16 kwietnia 1993 to grupa informacji biznesowej nieupublicznionej, potocznie zwana tajemnicami przedsiębiorstwa, dostępna określonym grupom lub pracownikom naszej firmy np. kadra kierownicza, zarząd, rada nadzorcza. Nieprawidłowe zarządzanie tą informacją podnosi ryzyko utraty kluczowych klientów, partnerów biznesowych, technologii, kradzież wartości intelektualnych.

Jakie cechy powinna posiadać informacja, będąca tajemnicą przedsiębiorstwa, żeby można było zastosować przepisy ustawy w stosunku do np. nieuczciwego pracownika ?

ma charakter informacji technicznej, technologicznej, organizacyjnej lub innej posiadającej wartość gospodarczą nie została ujawniona do wiadomości publicznej podjęto w stosunku do niej niezbędne działania w celu zachowania poufności.

Przykłady informacji mogącej stanowić tajemnice przedsiębiorstwa:

- działania marketingowe, w tym pozyskiwanie klientów
- stan i struktura jednostki
- zasady finansowe, wysokości wynagrodzeń
- powiązania kapitałowe nie udostępniane kontrahentom
- źródła zaopatrzenia i zbytu
- stopień wykorzystania mocy produkcyjnych
- lista odbiorców usług

Sankcje karne

Maksymalną karą przewidzianą za naruszenia prawa ochrony informacji lub ochrony danych osobowych jest kara ograniczenia wolności albo pozbawienia wolności do lat 3. (ustawa o ochronie danych osobowych art. Art. 49 do 54 lub kodeks karny art. 266-269). Przewidywane kary w unijnym projekcie zmian w ustawie sięgają miliona euro lub 2% obrotów. Bardziej niż kar wynikających z przepisów karnych należałoby się obawiać strat z powodu utraty wizerunku w przypadku niewłaściwego lub bezprawnego przetwarzania lub utraty informacji.

Podsumowanie

W artykule przedstawiono podstawowy podział informacji wynikający z przepisów prawa, ogólne obowiązki i zagrożenia nieodpowiedniego przetwarzania informacji w szczególności danych osobowych. Nie omówiono informacji niejawnych, a także szczegółowych ustaw branżowych czy tajemnicy lekarskiej, które prawdopodobnie czytelnikom są znane.

Należy zauważyć że tematyka ochrony informacji jest coraz bardziej popularna. Wartość informacji wzrasta, co skutkuje wydatkami na poprawę bezpieczeństwa. W ostatnich latach powstały normy wspomagające zarządzanie bezpieczeństwem informacji jak ISO/IEC 27001 i szereg norm powiązanych. Warto skorzystać z rozwiązań w tej dziedzinie.

fotki do zrobienia lub dental XP