MGR INŻ. TOMASZ RADZISZEWSKI

PERSPEKTYWA INFORMATYZACJI DZIAŁALNOŚCI PODMIOTÓW PRZETWARZAJĄCYCH DANE OSOBOWE PACJENTÓW

1. Wstęp

W dynamicznie rozwijającym się społeczeństwie jednym z głównych „surowców" wykorzystywanych do napędzania procesów rozwoju gospodarczego i społecznego stała się informacja. Synteza wcześniej zdefiniowanych teorii dot. społeczeństwa i zachodzących w nim „burzliwych" zmian oraz informacji jako zasobu doprowadziła do zdefiniowania teorii społeczeństwa informacyjnego, którego jedną z charakterystycznych cech jest narastający głód informacji[1].

Wraz ze wzrostem agresywnej eksploatacji tego zasobu objawiło się wyraźnie zarysowane zjawisko polaryzacji norm koegzystencji na linii: jednostka – państwo, pracownik – pracodawca, uczeń – nauczyciel, czy też sprzedawca – klient.

W obowiązującym porządku konstytucyjnym[2] status informacyjny jednostki został zdefiniowany wachlarzem praw pozytywnych gwarantujących jednostce: prywatność i ochronę życia rodzinnego, tajemnicę i swobodę komunikowania się, decydowanie o swoim życiu osobistym, ochronę zdrowia oraz prawem o charakterze negatywnym zabraniającym władzom publicznym pozyskiwania, gromadzenia i udostępniania innych informacji niż niezbędne w demokratycznym państwie prawnym[3] (prawa sytuowane art. 47, 49, 51, 68 ust. 1 Konstytucji RP).

Zdefiniowane za pomocą tych praw granice autonomii jednostki dają jej m.in. możliwość zarządzania tą sferą, która związana jest z „udostępnianiem na zewnątrz" informacji, których nieautoryzowane ujawnienie mogłoby spowodować daleko idącą ingerencję w prywatność. Postulat ten odnosi się do informacji związanych m.in.: ze stanem zdrowia, relacjami rodzinnymi, czy też sytuacją ekonomiczną, te zaś bezsprzecznie kształtują sferę prywatności „jednostki-pacjenta".

Określona ustawą o prawach pacjenta i Rzeczniku Praw Pacjenta[4] definicja czyni 'pacjentem' osobę, która zwraca się o udzielenie świadczeń zdrowotnych lub korzystającą ze świadczeń zdrowotnych udzielanych przez podmiot udzielający świadczeń zdrowotnych lub osobę wykonująca zawód medyczny.

Wynikająca z tej definicji interakcja oparta jest na realizacji praw pacjenta oraz obowiązkach związanych z udzielaniem świadczeń zdrowotnych przez świadczeniodawcę, których realizacja powinna uwzględnić ochronę informacji niezbędnych w procesie realizacji świadczeń zdrowotnych, jak i informacji uzyskanych „przy okazji", a dotyczących innych sfer życia prywatnego pacjenta[5,6], pozyskanych podczas ubiegania się o realizację świadczenia, jak i w trakcie jego realizacji.

Informacjami niezbędnymi w procesie realizacji świadczeń zdrowotnych mogą być te ogólnie definiujące stan zdrowia, jak i te o: kontaktach i preferencjach seksualnych, kodzie genetycznym, nałogach, podlegające również ochronie na mocy art. 27 ustawy o ochronie danych osobowych[7,8].

Należy zauważyć, iż obowiązek ochrony danych osobowych pacjenta rozciąga się również na działania związane z ich wtórnym przetwarzaniem przez organy i instytucje oraz upoważnione ustawą inne podmioty (np. samorząd lekarski, NFZ, ZUS itd), które nie biorą bezpośredniego udziału w procesie realizacji świadczenia zdrowotnego, a realizują przetwarzanie informacji, do ochrony których podmioty te są zobowiązane na mocy lex specialis oraz ustawy o ochronie danych osobowych.

Procedury przetwarzania informacji pozyskanych podczas zwracania się o udzielenie świadczeń zdrowotnych, korzystania ze świadczeń zdrowotnych lub wtórnego przetwarzania tych informacji składają się na model ochrony danych osobowych pacjenta funkcjonujący w niezwykle szerokim obszarze normowania[9], dlatego podjęta w niniejszym opracowaniu tematyka uległa ograniczeniu.

---

[1] T. Białobłocki , J. Moroz, M. Nowina-Konopka, L. W. Zacher, *Społeczeństwo informacyjne. Istota, problemy, wyzwania*, Warszawa 2006.

[2] Konstytucja Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. 1997 nr 78 poz. 483. ze zm.).

[3] M. Jabłoński (red.), *Wolności i Prawa Jednostki w Konstytucji RP. Tom I Idee i Zasady Przewodnie Konstytucyjnej Regulacji Wolności i Praw Jednostki w RP*, Warszawa 2010.

[4] Dz.U. 2009.52.417 ze zm.,

[5] Patrz art. 14 ust. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, art. 40 ustawy o zawodach lekarza i lekarza dentysty, art. 21 ustawy o zawodach pielęgniarki i położnej.

[6] D. Karkowska, *Ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta. Komentarz,* Warszawa 2010.

[7] Dz.U. 2002.101.926 ze zm.

[8] Perspektywa ochrony informacji uzyskanych „przy okazji" jest kształtowana (w zależności od ich kategorii) na podstawie art. 27 lub 23 ustawy o ochronie danych osobowych.

[9] W tym przypadku oprócz tzw. „białych ustaw i rozporządzeń" mają również zastosowanie wymagania prawne związane m.in. z informatyzacją działalności podmiotów realizujących zadania publiczne, prawem pracy, działalnością ubezpieczeniową, działalnością organów ochrony państwa itd.) Np.: Ustawa o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi (Dz. U. 2007.70.473 ze zm.); Ustawa o Państwowej Inspekcji Sanitarnej (Dz.U. 2006.122.851 ze zm.); Ustawa o Rzeczniku Praw Obywatelskich (Dz.U. 2001.14.147 ze zm.); Ustawa o Rzeczniku Praw Dziecka (Dz.U. 2000.6.69 ze zm.); Ustawa o policji (Dz.U. 2007.43.277 ze zm.); Ustawa o ochronie danych osobowych (Dz.U. 2002.101.926 ze zm.); Ustawa i prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. 2009.52.417 ze zm.); Ustawa przepisy wprowadzające ustawę o prawach pacjenta i Rzeczniku Praw Pacjenta, ustawę o akredytacji w ochronie zdrowia oraz ustawę o konsultantach w ochronie zdrowia (Dz.U. 2009.76.641 ze zm.); Ustawa o zakładach opieki zdrowotnej (Dz.U. 2007.14.89 ze zm.); Ustawa o ochronie zdrowia psychicznego (Dz.U. 1994.111.535 ze zm.); Ustawa o planowaniu rodziny, ochronie płodu ludzkiego i warunkach dopuszczalności przerywania ciąży (Dz.U nr 17 poz. 78 ze zm.); Ustawa o zawodach lekarza i lekarza dentysty (Dz.U. 2008.136.857 ze zm.); Ustawa o lekarzu sądowym (Dz.U. 2007.123.849 ze zm.); Ustawa o zawodach pielęgniarki i położnej (Dz.U. 2009.151.1217 ze zm.); Ustawa o zawodzie psychologa i samorządzie zawodowym psychologów (Dz.U. 2001.763 ze zm.); Ustawa o zawodzie felczera (Dz.U. 2004.53.531 ze zm.); Ustawa z dnia 22 sierpnia 1997r. o publicznej służbie krwi (Dz.U. 1997.106.681 ze zm.); Ustawa o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych (Dz.U. 2008.14.92 ze zm.); Ustawa Prawo Farmaceutyczne (Dz.U. 2001.126.1381 ze

Artykuł stanowi próbę przedstawienia podstawowych założeń obowiązującego modelu ochrony danych osobowych pacjenta przyjmując perspektywę przetwarzana danych w systemach teleinformatycznych, koncentrując się na aspektach praktyki stosowania obowiązujących przepisów prawa i dostrzeganych zagrożeniach wynikających z planowanych w tym zakresie normowań.

Podjęta próba bazuje na praktyce stanowienia i wdrażania wewnętrznych standardów ochrony danych osobowych[10].

Opracowanie stanowi również próbę zabrania głosu w toczącej się dyskusji nt. realizacji procesów informatyzacji działalności podmiotów realizujących zadania publiczne, próbując rzucić dyskretne światło na płaszczyznę rozwiązań zarządczych warunkujących skuteczność i racjonalność funkcjonowania techniczno – prawnych środków ochrony informacji. Istnienie tej płaszczyzny jest w literaturze prawnej w sposób widoczny pomijane.

Zdefiniowanie perspektywy informatyzacji przetwarzania danych osobowych pacjenta było podyktowane również przyjęciem przez autora opracowania postulatu, na mocy którego należy uznać, iż rozwój społeczeństwa informacyjnego jest realizowany w oparciu o wykorzystywanie różnorodnych technik informacyjnych opartych w dużej mierze na infrastrukturze teleinformatycznej, a eksploatacja tego zasobu stanowi źródło największych zagrożeń dla realizacji podstawowych praw i wolności jednostki.

2. Systemowe podejście do ochrony danych osobowych pacjentów

W celu zobrazowania tych problemów poddajmy analizie pewien zasób wymagań prawnych związanych z ochroną danych osobowych pacjentów przetwarzanych w systemach teleinformatycznych, próbując dokonać translacji języka norm prawnych na język procedur operacyjnych:

1. Art. 36 ust. 1, 3, art. 39a. ustawy o ochronie danych osobowych;
2. § 73, 86 ust. 2 Rozporządzenia MZ w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania[11];
3. § 14 ust. 1 projektu Rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w formie elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (podmiotów realizujących zadania publiczne).

Rozporządzenie MSWiA z dnia 29 kwietnia 2004 r.[12] stanowiące rozwiązanie delegacji art. 39a u.o.d.o stanowi próbę ustalenia poziomów minimalnych zabezpieczeń[13]. Z punktu widzenia poniesionych na ich wdrożenie kosztów i osiągniętej minimalnej zgodności można ulec złudzeniu, że problem zabezpieczeń po wdrożeniu wymagań wynikających z Rozporządzenia technicznego został rozwiązany. Tymczasem ustawodawca „znacznie komplikuje" sposób realizacji wymagań Rozporządzenia technicznego na płaszczyźnie techniczno - organizacyjnej na podstawie przepisu który stanowi, że administrator danych osobowych powinien „zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń" (art. 36 ust. 1 u.o.d.o)

Analiza incydentów związanych z ochroną danych osobowych[14] buduje przekonanie, iż implementacja wymagań techniczno – organizacyjnych zawartych w Rozporządzeniu technicznym nie daje rękojmi skutecznej ochrony danych i potwierdza zamysł ustawodawcy, aby wymagania te stanowiły punk wyjścia – obligatoryjny poziom podstawowy, dając jednocześnie podmiotom zobowiązanym w art. 36 ust. 1 u.o.d.o podstawę do budowania komplementarnych do kultury organizacyjnej zabezpieczeń techniczno – organizacyjnych, nakazując jednocześnie ich stosowanie pod rygorem art. 51 u.o.d.o.

Per analogiam można odczytać intencje prawodawcy, związane z zabezpieczaniem danych osobowych pacjentów w systemach IT zaimplementowane w § 86 ust. 2 pkt. 1, 3 Rozporządzenia MZ w sprawie rodzaju i zakresu dokumentacji medycznej…[15], a § 86 ust. 1 pkt. 3 kreuje imperatyw nadążania za zmianami technologicznymi, co buduje oczywisty kontekst dla analizy zagrożeń[16] i podatności[17] (w tym wypadku nie ulega wątpliwości, iż procedury analizy powinny być prowadzone wg określonych procedur operacyjnych w celu zapewnienia odpowiedniej jakości i wiarygodności uzyskanych tą droga danych).

Podstawa powołania Administratora Bezpieczeństwa Informacji zdefiniowana art. 36 ust. 3 u.o.d.o. stwarza pozornie niewielkie możliwości translacyjne na język procedur operacyjnych, ponieważ na jego podstawie administrator danych może, ale nie musi, powołać Administratora Bezpieczeństwa Informacji (ABI) i to tyle, jeśli chodzi o samą wykładnię.

zm.); Ustawa o diagnostyce laboratoryjnej (Dz.U. 2004.144.1529 ze zm.); Ustawa o izbach aptekarskich (Dz.U. 2008.136.856 ze zm.); Ustawa o izbach lekarskich (Dz.U. 2009.219.1708); Ustawa o samorządzie pielęgniarek i położnych (Dz.U. nr 41.178 ze zm.); Ustawa o konsultantach w ochronie zdrowia (Dz.U. 2009.52.419 ze zm.); Ustawa o Państwowym Ratownictwie Medycznym (Dz.U. 2006.191.1410 ze zm.); Ustawa o nadzorze ubezpieczeniowym i emerytalnym oraz Rzeczniku Ubezpieczonych (Dz.U. 2003.124.1153 ze zm.); Ustawa o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz.U. 2008.164.1027 ze zm.); Ustawa o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów (Dz.U. 2005.169.1411 ze zm.); Ustawa o przeciwdziałaniu narkomanii (Dz.U. 2005.179.1485 ze zm.); Ustawa o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi (Dz.U. 2008.234.1570 ze zm.); Ustawa o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz.U. 2009.153.1227 ze zm.); Ustawa o akredytacji w ochronie zdrowia; Ustawa Kodeks Pracy (Dz.U. 1998.21.94 ze zm.);

1. Ustawa Kodeks cywilny (Dz.U. 1964.16.93 ze zm.); Ustawa Kodeks postępowania administracyjnego (Dz.U. 2000.98.1071 ze zm.); Ustawa Kodeks postępowania cywilnego (Dz.U. 1964.43.296 ze zm.); Ustawa Kodeks rodzinny i opiekuńczy (Dz.U. 1964.9.59 ze zm.); Ustawa Kodeks karny wykonawczy (Dz.U. nr 90 poz. 557 ze zm.);

2. Ustawa Prawo o ruchu drogowym (Dz.U. 2005.108.908 ze zm.); Ustawa o działach administracji rządowej (Dz.U. 2007.65.437 ze zm.); Ustawa o samorządzie gminnym (Dz.U. 2001.142.1591 ze zm.); Ustawa o samorządzie powiatowym (Dz.U. 2001.142.1592 ze zm.); Ustawa o samorządzie wojewódzkim (Dz.U. 2001.142.1590 ze zm.); Ustawa o wojewodzie i administracji rządowej w województwie (Dz.U. 2009.31.206 ze zm.) oraz wynikające z nich przepisy aktów wykonawczych.

[10] Kształtowanej na podstawie wieloletniej praktyki zawodowej autora opracowania prowadzącego działalność ekspercką w dziedzinie ochrony informacji pod nazwą 5de management systems.

[11] Zwanego dalej Rozporządzeniem ws dokumentacji medycznej (Dz.U. 2010.252.1697).

[12] W sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych - zwanego w tekście Rozporządzeniem technicznym (Dz. U. 2004.100.1024).

[13] Co zresztą zostało wyartykułowane w § 1 pkt. 2 Rozporządzenia MSWiA z 29 kwietnia 2004 r., który mówi o podstawowych warunkach techniczno – organizacyjnych.

[14] Na podstawie doświadczeń autora artykułu.

[15] § 86 ust. 2 „Zabezpieczenie dokumentacji prowadzonej w postaci elektronicznej wymaga w szczególności:

1) systematycznego dokonywania analizy zagrożeń; (…)

2) stosowania środków bezpieczeństwa adekwatnych do zagrożeń".

[16] Definiowanych jako potencjalne przyczyny niepożądanego zdarzenia, które mogą wywołać szkodę w procesie lub zasobach systemu.

[17] Definiowanych jako słabości procesu lub zabezpieczeń systemu, które mogą zostać wykorzystanie przez zagrożenia.

Jeśli spojrzymy na problem z perspektywy zarządczej, to można dostrzec konieczność stworzenia funkcjonalnej struktury organizacyjnej związanej z zarządzaniem ochroną danych osobowych, opartej na podziale na funkcje zarządcze (np. gestorzy zasobu informacyjnego, administratorzy systemów przetwarzania) oraz kontrolne (np. ABI, który powinien posiadać określone kompetencje[18], ABS – administrator bezpieczeństwa systemu IT), takie podejście wymaga jednak rozwiązania adekwatnego do posiadanych zasobów.

Analiza przedstawionego wcześniej zasobu wymagań prawnych związanych z ochroną danych osobowych pacjentów daje możliwość odniesienia się również do problemu archiwizacji danych. Realizacja minimalnego poziom zabezpieczeń wymaga stosowania procedur operacyjnych związanych z archiwizacją zapewniających jej realizację w odpowiednich warunkach i pod nadzorem zapewniającym danym poufność, integralność oraz dostępność[19] (która powinna być skorelowana z ustawowym czasem przechowywania dokumentacji zawierającej dane osobowe pacjentów[20] oraz 24 godzinnym dostępem do dokumentacji przekazanej do archiwum zakładowego lub zakładowej składnicy akt). W tym obszarze ustawodawca pozostawia po raz kolejny „dużo swobody" w doborze i stosowaniu metod i środków ochrony dokumentacji, co w praktyce nastręcza placówkom opieki zdrowotnej wiele problemów:

1. związanych ze stworzeniem adekwatnych warunków w pomieszczeniach zakładowych archiwów/składnic akt[21] gwarantujących:
   a. właściwą temperaturę i wilgotność powietrza,
   b. odpowiednie sztuczne oświetlenie,
   c. brak agresywnego chemicznie oddziaływania powłok znajdujących się na ścianach i wyposażeniu pomieszczenia,
   d. minimalizację wpływu wody pochodzącej z instalacji wod-kan,
   e. eliminację szkodliwej flory i fauny,
   f. monitoring ppoż.
2. związanych z analizą stanu nośników papierowych, z tworzyw sztucznych (wywołane błony RTG, wydruki na kliszy RTG) i magnetooptycznych (biorąc pod uwagę ich trwałość) w kontekście obowiązku czasowego ich przechowywania;
3. związanych z bezpiecznym niszczeniem dokumentacji po ustawowym okresie jej przechowywania;
4. związanych z procedurami wydawania dokumentacji (również na zewnątrz[22]) i przyjmowania dokumentacji po jej wykorzystaniu.

Jako próbę (o charakterze poszerzającym) implementacji zasad związanych z archiwizacją danych osobowych pacjentów, zawartych w dokumentacji medycznej można potraktować stosowanie wymagań akredytacyjnych opracowywanych przez Centrum Monitorowania Jakości w Ochronie Zdrowia na podstawie ustawy z dnia 6 listopada 2008 w sprawie akredytacji w ochronie zdrowia. Zasięg ich stosowania jest jednak ograniczony biorąc pod uwagę dobrowolność poddawania się procedurze akredytacyjnej przez podmiot udzielający świadczeń zdrowotnych, a sytuacji nie poprawia dodatkowe punktowanie na rzecz świadczeniobiorcy za uzyskanie certyfikatu akredytacyjnego podczas procedury kontraktowania świadczeń przez NFZ.

Ocena zatwierdzonych przez Radę Akredytacyjną standardów akredytacyjnych w obszarze Zarządzania Informacją (ZI) i wynikających z nich wymagań związanych z archiwizacją danych nie jest jednak jednoznaczna i zawiera krytyczne uwagi.

Standard wprowadza konieczność monitorowania wilgotności i temperatury powietrza w pomieszczeniu archiwum, w którym przechowywana jest dokumentacja medyczna na nośniku papierowym[23], nie znajdziemy w nim jednak konsekwentnego odniesienia do zasad monitorowania w/w parametrów w odniesieniu do nośników elektronicznych, dla których szczególnie wilgotność (dla nośników magnetycznych) wprowadza ograniczenia ich przydatności do długotrwałego przechowywania danych.

Zasady realizacji monitoringu zawarte w standardzie akredytacyjnym powinny zostać doprecyzowane wartościami granicznymi pozwalającymi na dokonanie oceny jakościowej środowiska przechowywania nośników papierowych i magnetooptycznych (np. wartości graniczne natężenia światła, wilgotności i temperatury).

W praktyce podmioty lecznicze przystępujące do nadzoru akredytacyjnego, lub wdrażające przy innej okazji wewnętrzne standardy przechowywania definiują procedury operacyjne w oparciu o wartości graniczne określone w Rozporządzeniu w sprawie warunków przechowywania dokumentacji osobowej i płacowej pracodawców[24] lub w oparciu o znacznie ostrzejsze kryteria ustalone przez prawodawcę w Rozporządzeniu w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych[25].

W tym przypadku rodzi się kwestia podstaw finansowania stosowanych rozwiązań wynikających z w/w przepisów wykonawczych. Wydaje się zasadnym, iż poniesione przez publiczne podmioty lecznicze (niebędące podmiotem w/w Rozporządzenia ws instrukcji kancelaryjnej) nakłady finansowe na przechowywanie dokumentacji w formie elektronicznej mogą mieć uzasadnienie w sformułowanej przez prawodawcę dyrektywie stosowania metod i środków ochrony, których skuteczność w czasie ich zastosowania jest powszechnie uznawana[26]. Przyjęcie takiego podejścia posiada również racjonalne uzasadnienie ze

[18] Autor opracowania stoi na stanowisku, że pojęcie kompetencji odnosi się do wykształcenia, doświadczenia i uprawnień zarządczych w tym przypadku pozwalających na realizację zadań przypisanych dla administratora danych osobowych.

[19] Patrz § 73 oraz § 80 pkt. 1, 2, 3 Rozporządzenia MZ w sprawie rodzajów i zakresu dokumentacji medycznej w zakładach opieki zdrowotnej oraz sposobu jej przetwarzania.

[20] Art. 29 Ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. 2009.52.417).

[21] Utworzenie zakładowego archiwum (w państwowych jednostkach organizacyjnych, jednostkach samorządu terytorialnego, w których powstają materiały archiwalne w myśl art. 1 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach zwanej dalej u.z.n.a. (Dz.U. 2011.123.698 ze zm.)) jest sankcjonowane decyzją Naczelnego Dyrektora Archiwów Państwowych lub właściwego dyrektora archiwum państwowego (patrz art. 33 u.z.n.a). W innych przypadkach w państwowych i samorządowych jednostkach organizacyjnych kierownik tej jednostki tworzy zakładową składnicę akt (patrz art. 36 u.z.n.a).

[22] Np. na podstawie art. 26 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta.

[23] Punkt ZI 3.2 Zestawu standardów akredytacyjnych z lutego 2010.

[24] Rozporządzenie Ministra Kultury z dnia 15 lutego 2005, którego podmiotem jest organizacja prowadząca działalność w dziedzinie przechowywania dokumentacji, a zdefiniowane w Rozporządzeniu kryteria oceny wilgotności i temperatury środowiska przechowywania odnoszą się tylko do parametrów ochrony nośników papierowych (Dz.U.2005.32.283 i 284).

[25] Rozporządzenie Prezesa Rady ministrów z dnia 11 stycznia 2011 r. (zwane dalej Rozporządzeniem ws instrukcji kancelaryjnej), którego podmiotem są organy gminy i związków międzygminnych, organy powiatu, organy samorządu województwa i organy zespolonej administracji rządowej w województwie, urzędy obsługujących te organy (Dz.U. 2011.14.67), zdefiniowane w Rozporządzeniu wartości graniczne związane z monitoringiem temperatury, wilgotności odnoszą się również do informatycznych nośników danych, klisz filmowych, taśm filmowych i magnetycznych.

[26] Patrz §86 ust.1 pkt.3 Rozporządzenia ws instrukcji kancelaryjnej.

względu na nakreśloną w ustawie z dnia 18 kwietnia 2011 r. o systemie informacji w ochronie zdrowia perspektywie digitalizacji dokumentacji medycznej[27].

Rozpatrywana przestrzeń wymagań prawnych zawiera więcej pytań niż odpowiedzi w płaszczyźnie techniczno – organizacyjnej. Konieczność ich stosowania wymusza jednak działania placówek ochrony zdrowia, które ze względu na specyfikę ich funkcjonowania nie powinny być w żadnym wypadku chybione, szczególnie ze względu na koszty oraz ryzyka prawne, których materializację należy rozpatrywać również na płaszczyźnie gospodarowania środkami publicznymi.

Odpowiedź na pytanie jak zdefiniować „właściwy", „odpowiedni", „powszechnie uznawany za skuteczny" poziom zabezpieczeń była zawarta w § 3 ust. 2 uchylonego w grudniu 2010 r. Rozporządzenia Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych (podmiotów realizujących zadania publiczne)[28] a obecnie w §14 ust. 1 projektu Rozporządzenia w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w formie elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

W tym wypadku prawodawca stawiając to wymaganie nakreślił właściwy kierunek na płaszczyźnie organizacyjnej, który pozwoli na racjonalne i skuteczne zarządzanie bezpieczeństwem danych osobowych pacjentów, w oparciu o standard PN-ISO/IEC 27001:2007[29,30] i standardy z nim związane: PN-ISO/IEC 27005:2010[31], PN-ISO/IEC 24762:2010[32] oraz PN-ISO/IEC 17799:2007[33]. Standardy te stwarzają kontekst zarządzania ochroną informacji w oparciu o podejście procesowe[34] i zarządzenie ryzykiem[35].

W praktyce, możliwość stosowania komplementarnych rozwiązań ochrony danych stworzona na podstawie przepisów wykonawczych dot. m.in. zakresu i zasad przetwarzania dokumentacji medycznej, Krajowych Ram Interoperacyjności i wymagań dla systemów teleinformatycznych podmiotów realizujących zadania publiczne[36], instrukcji kancelaryjnej i zasad funkcjonowania archiwów zakładowych, generuje jednak szereg zagrożeń. Charakter tych zagrożeń związany jest z wymogiem stosowania w całości wspominanych wcześniej międzynarodowych standardów[37], co może spowodować głęboką ingerencję w realizację procesów biznesowych i statutowych. Zakres standardów przewiduje oprócz implementacji podejścia procesowego, m.in. konieczność opracowania, wdrożenia, utrzymywania i doskonalenia procedur związanych z nadzorowaniem tzw. działań korygujących i zapobiegawczych, audytu wewnętrznego, nadzoru nad incydentami, nadzorowania dokumentów i zapisów, procedur nadzorowania ciągłości działania (BCM), zarządzania usługami dostarczanymi przez strony trzecie.

Nadzorowania w ramach wytycznych standardów wymaga również środowisko systemów teleinformatycznych między innymi w zakresie:

a. bezpieczeństwa fizycznego sprzętu IT (rozdział A 9.2[38]);
b. procedur eksploatacyjnych sprzętu IT i zakresów odpowiedzialności za te procedury (A 10.1);
c. planowania i odbiorów systemów IT (A 10.3);
d. ochrony przed kodem złośliwym i mobilnym (A 10.4);
e. realizacji kopii zapasowych (A 10.5);
f. zabezpieczania sieci (A 10.6), kontroli dostępu do sieci (A.11.4);
g. obsługi nośników (A 10.7);
h. monitorowania systemu (A 10.10);
i. wymagań biznesowych wobec kontroli dostępu (A 11.1);
j. zarządzania dostępem użytkowników (A.11.2)
k. odpowiedzialności użytkowników (A.11.3)
l. kontroli dostępu do systemów operacyjnych (A.11.5)
m. kontroli dostępu do aplikacji (A.11.6)
n. przetwarzania mobilnego i pracy na odległość (A.11.7)
o. poprawnego przetwarzania w aplikacjach (A.12.2)
p. zabezpieczenia kryptograficznego (A.12.3)
q. bezpieczeństwa plików systemowych (A.12.4)
r. bezpieczeństwa w procesach rozwojowych i obsługi informatycznej (A.12.5)

Dotychczasowe doświadczenia pozwalają sądzić, iż na umiarkowanie uprzywilejowanej pozycji znajdują się placówki ochrony zdrowia posiadające wdrożone wewnętrzne standardy np. zarządzania jakością, środowiskiem oraz bezpieczeństwem i higieną pracy zgodne z ISO 9001, ISO 14001 oraz ISO 18001[39], jak i

[27] Patrz art. 56 ust. 1 ustawy.

[28] „Przy opracowywaniu polityki bezpieczeństwa, o której mowa w ust. 1, podmiot publiczny (również realizujący zadania publiczne – przyp. autora) powinien uwzględniać postanowienia Polskich Norm z zakresu bezpieczeństwa informacji".

[29] PN-ISO/IEC 27001:2007 „Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania".

[30] Przepis § 3 ust. 2 uchylonego rozporządzenia - Rozporządzenia Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych stwarzał możliwość stosowania dedykowanego dla służby zdrowia standardu PN-EN ISO 27799:2008 „Informatyka w ochronie zdrowia. Zarządzanie bezpieczeństwem informacji w ochronie zdrowia przy użyciu ISO 27002 oraz PN-ISO/IEC 27001:200727" opracowany przez PKN w KT 302 ds. Zastosowania Informatyki w Ochronie Zdrowia, pozostaje więc kwestią nierozstrzygniętą czy normę PN-EN ISO 27799:2010 można traktować jako normę uzupełniającą standard PN-ISO/IEC 27001:2007 i posiadającą tym samym status obowiązującej do wdrożenia w odniesieniu do systemów teleinformatycznych.

[31] PN-ISO/IEC 27005:2010 „Technika informatyczna - Techniki bezpieczeństwa - Zarządzenie ryzykiem w bezpieczeństwie informacji".

[32] PN-ISO/IEC 24762:2010 „Technika informatyczna - Techniki bezpieczeństwa - Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie".

[33] PN-ISO/IEC 17799:2007 „Technika informatyczna - Techniki bezpieczeństwa - Praktyczne zasady zarządzania bezpieczeństwem informacji" - standard stanowiący podręcznik stosowania zabezpieczeń opisanych w załączniku normatywnym A standardu PN-ISO/IEC 27001:2007; z dużym przybliżeniem można użyć stwierdzenia, iż jest to poprzednik, a zarazem polski odpowiednik standardu ISO/IEC 27002:2007.

[34] W oparciu o PN-EN ISO 9001:2009 należy założyć, iż w celu skutecznego działania organizacja powinna zidentyfikować pozostające w ścisłym związku działania i nimi zarządzać, tak aby niezbędne do ich realizacji zasoby (tzw. wejścia) przekształcić w zamierzony wynik (wyjścia). Przekształcanie „wejścia" w „wyjścia" można rozpatrywać jako proces, którego wynik może stanowić „wejścia" do innego procesu. Stosowanie identyfikacji procesów oraz sterowanie ich wzajemnym oddziaływaniem w celu osiągnięcia zamierzonego wyniku można definiować jako „podejście procesowe".

[35] Na podstawie art. 2 pkt. 17 ustawy o ochronie informacji niejawnych (Dz.U.2010.182.1228) zarządzanie ryzykiem to skoordynowane działania w zakresie zarządzania bezpieczeństwem informacji z uwzględnieniem ryzyka.

[36] Mowa o projekcie rozporządzenia Rady Ministrów ws. Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w formie elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych przygotowywanego na podstawie delegacji art. 18 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, wcześniejsze rozporządzenie w sprawie minimalnych wymagań dla systemów teleinformatycznych z dnia 11 października 2005 zostało uchylone z dniem 16 grudnia 2010 r.

[37] Prawodawca nie wskazał możliwości jakichkolwiek wyłączeń, poza tymi których wyłączenie jest uzasadnione wynikami procesu szacowania ryzyka (dot. PN-ISO/IEC 27001:2007, nie mniej jednak mogą one odnosić się tylko do celów i środków zabezpieczania przedstawionych w załączniku normatywnym „A" tego standardu).

[38] Oznaczenie dotyczy rozdziałów „Załącznika normatywnego A" i stanowi zarazem odesłanie do odpowiedniego rozdziału normy PN ISO/IEC 17799:2007 podlegającego tej samej numeracji, jednak bez litery „A".

[39] Mowa o standardach: PN-EN ISO 9001:2009 Systemy zarządzania jakością - Wymagania, PN-EN ISO 14001:2005 Systemy zarządzania środowiskowego - Wymagania i wytyczne

realizujące procedury kontroli zarządczej zdefiniowanej ustawą o finansach publicznych.

W tym przypadku wydaje się, iż najlepszym rozwiązaniem byłaby budowa zintegrowanych systemów zarządzania spełniających wymagania wcześniej wspomnianych standardów zarządzania jakością, środowiskiem, bezpieczeństwem i higieną pracy oraz bezpieczeństwem informacji, co wymaga jednak wiedzy eksperckiej z zakresu samych standardów, specyfiki funkcjonowania podmiotów realizujących zadania dot. ochrony zdrowia (w tym mających zastosowanie wymagań prawnych), jak i zasobów gwarantujących uzyskanie odpowiedniego poziomu technologicznego.

W pozostałych przypadkach, gdy implementacja (do porządku organizacyjnego zobowiązanych podmiotów), przyjętego w polskim porządku prawnym modelu bezpiecznego przetwarzania informacji o pacjencie nie będzie realizowana w oparciu o posiadane doświadczenia dotyczące zarządzania ryzykiem oraz tzw. zarządzania procesowego, zmiany zachodzić będą znacznie wolniej i mniej skutecznie.

W przypadku podmiotów dysponujących ograniczonym wachlarzem zasobów (np. indywidualne praktyki lekarskie, pielęgniarskie) spełnienie wymagań prawnych stanowić będzie znaczne wyzwanie organizacyjne, którego głównym celem powinno być osiągnięcie stanu homeostazy parametrów dot. kosztów i skuteczności zabezpieczania przy jednoczesnym spełnieniu minimalnych warunków wynikających z przepisów prawa.

Należy się spodziewać, iż przy obecnym stanie świadomości, wiedzy, doświadczenia, oraz kultury technologicznej, rezultaty w postaci wzrostu bezpieczeństwa i racjonalności procedur przetwarzania danych o pacjencie (w wyniku wprowadzonych i planowanych do porządku prawnego zmian), mogą być obserwowalne w perspektywie kilku lub nawet kilkunastoletniej. Punkt odniesienia dla tego postulatu tworzy m.in. ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia, która zakłada od 31 lipca 2014 r. przetwarzanie dokumentacji medycznej tylko w formie elektronicznej[40].

3. Paradygmat[41] prawno-techniczny zabezpieczania danych osobowych pacjentów

Odwołując się do doświadczeń można uznać, iż reengineering[42] procesów związanych z ochroną danych osobowych pacjentów jest w większości przypadków właściwie jedyną drogą budowania standardów ochrony informacji ze względu na głęboko zakorzeniony paradygmat kształtujący ochronę danych jako problem wyłącznie natury prawnej i technicznej.

W tej sytuacji wydaje się, iż warunkiem niezbędnym dla powodzenia reengineeringu jest metanoia[43], której powinno doświadczać najwyższe kierownictwo, w celu zainicjowania i wspierania wszystkich działań związanych z wdrożeniem elastycznego, skutecznego i racjonalnego podejścia do ochrony danych osobowych.

Na paradygmat techniczno – prawny składa się utożsamianie (na zasadach postawienia znaku równości) zabezpieczania[44] informacji z ochroną systemów teleinformatycznych, marginalizując tym samym rolę personelu, który w tym przypadku jest fundamentem systemu informacyjnego, w skład którego, oprócz infrastruktury teleinformatycznej, wchodzą inne kanały informacyjne oparte np. na mowie, dźwięku, geście, znaku odręcznie pisanym.

W praktyce mamy do czynienia zatem z heterogenicznym i rozproszonym systemem przetwarzania, którego skuteczność i elastyczność jest ściśle uzależniona od świadomego uczestnictwa w funkcjonowaniu zabezpieczeń wszystkich członków organizacji. Wzmocnienie tego kryterium można uzyskać poprzez wymaganie w stosowaniu zabezpieczeń[45] udziału dostawców, pacjentów oraz wykorzystywanie specjalistycznego doradztwa osób spoza organizacji i pozytywnych praktyk benchmarkingowych[46].

Kolejną składową paradygmatu, stanowiącą przeszkodę w budowaniu skutecznych i racjonalnych rozwiązań jest postrzeganie bezpieczeństwa jako stanu pomiędzy incydentami. Doskonalenie przyjętych rozwiązań ma wówczas charakter reaktywny i opiera się głównie na poczynionych post factum wnioskach, często wynikających z własnych negatywnych doświadczeń. Dodatkowo, stosowane zabezpieczenia posiadają, nader często, charakter „statyczny". Jako przykład można przedstawić przepisy regulaminów organizacyjnych, regulaminów pracy, polityk bezpieczeństwa, które są rzadko aktualizowane i powstają w oparciu o wymagania umieszczane w dokumentacji innych organizacji, tworząc tym samym powszechnie powielany standard (np. na podstawie metodyki TISM[47]), nie odzwierciadlający kultury organizacyjnej podmiotu odpowiedzialnego za ochronę danych. Mechanizm oddziaływania takich zabezpieczeń często bazuje na strachu pracowników przed odpowiedzialnością karną i służbową.

Przeciwwagą do tego typu praktyk powinny być działania wdrażające zabezpieczenia zdefiniowane na podstawie procesu szacowania ryzyk związanych z ochroną informacji, do którego danymi wejściowymi powinny być:

1. mające zastosowanie wymagania prawne;
2. informacje o zagrożeniach i podatnościach (m.in. determinowanych zmianami: w strukturze organizacyjnej (alokacja kompetencji), w technologii, celów biznesowych bądź statutowych;
3. dane związane z monitoringiem skuteczności już wdrożonych zabezpieczeń techniczno - organizacyjnych.

stosowania, PN-N-18001:2004 Systemy zarządzania bezpieczeństwem i higieną pracy - Wymagania.

[40] Ustawa sankcjonuje wzajemne udostępnianie dokumentacji medycznej, prowadzonej przez świadczeniodawców z wykorzystaniem Systemu Informacji Medycznej (SIM) który jest systemem teleinformatycznym służącym przetwarzaniu danych dotyczących udzielonych, udzielanych i planowanych świadczeń opieki zdrowotnej udostępnianych przez systemy teleinformatyczne usługodawców, danych osobowych i jednostkowych danych medycznych usługobiorców oraz danych umożliwiających wymianę dokumentów elektronicznych między usługodawcami i usługodawcami a płatnikami.

[41] Paradygmat: tu uważany za przyjęty sposób widzenia rzeczywistości w danej dziedzinie, doktrynie.

[42] Pod tym pojęciem kryje się koncepcja biznesowa polegająca na wprowadzaniu radykalnych zmian w procesach biznesowych, których celem jest osiągnięcie maksymalnej efektywności organizacji oraz redukcja kosztów.

[43] Matanoia (grec.): zmiana sposobu myślenia, dla Greków oznaczało transcendencję (meta – „poza", „ponad") umysłu (noia, pochodzące od nous – „umysł").

[44] Autor podziela pogląd, iż używanie pojęcia „bezpieczeństwa informacji" nadaje procesom ochrony informacji zbyt statyczny charakter (bazując na znaczeniu słowa „bezpieczeństwo"), zatem mając na uwadze burzliwość procesów biznesowych w otoczeniu i wnętrzu organizacji zasadnym jest stosowanie pojęcia „zabezpieczania" informacji.

[45] Tu jako „zabezpieczania" należy rozumieć środki o charakterze techniczno - organizacyjnym, których stosowanie ma na celu obniżenie ryzyka związanego z utratą poufności, integralności i dostępności danych osobowych.

[46] Głównym celem tych działań jest wymiana doświadczeń dot. analizowanego obszaru aktywności biznesowej pomiędzy podmiotami na co dzień z sobą niekonkurującymi, a zmagającymi się z analogicznymi problemami.

[47] Metodyka zarządzania bezpieczeństwem informacji opracowana i stosowana przez ENSI Sp. z o.o.

Takie podejście gwarantuje identyfikację odpowiedniego poziomu zabezpieczeń w odniesieniu do konkretnych zasobów informacyjnych, co spowoduje, iż organizacja poniesie tylko uzasadnione koszty wdrożenia zabezpieczeń.

W kręgach najwyższego kierownictwa pokutuje często przeświadczenie, iż przepływ informacji dot. incydentów związanych z ochroną informacji powinien być skutecznie kontrolowany, w sposób gwarantujący zacieśnienie kręgu poinformowanych o incydencie do najwyższego kierownictwa.

Na podstawie dotychczasowych doświadczeń wdrożeniowych standardów ochrony informacji należy sądzić, iż działania związane z obsługą incydentu wymagają zdefiniowania szerszego celu nadzorowania przepływu informacji o incydentach, ponieważ nade wszystko podstawą realizacji wszystkich założeń tworzących bezpieczeństwo informacji powinna być odpowiednia komunikacja:

a) w organizacji – pomiędzy jej pracownikami,
b) w otoczeniu – pomiędzy organizacją a podmiotami rynkowymi (klientami, dostawcami, instytucjami samorządowymi i innych).

Stąd też informowanie o incydentach i zdarzeniach związanych z ochroną informacji powinno się rozpatrywać na powyższych dwóch poziomach ogólności. Pierwszy z nich powinien budować kontekst wspierający efektywne propagowanie bezpieczeństwa wśród pracowników i kierownictwa, tworzyć podwaliny mechanizmów informowania o incydentach i zdarzeniach związanych z bezpieczeństwem informacji, zapewniając równocześnie odpowiednie mechanizmy sterowania szczegółowością przekazu[48] dla użytku służbowego. Generując równocześnie dane wykorzystywane do funkcjonowania wszechstronnego i adekwatnego systemu pomiarowego używanego do oceny jakości zarządzania ochroną informacji.

Efektywna komunikacja zewnętrzna powinna gwarantować transparentność działań związanych z bezpieczeństwem budując tym samym zaufanie partnerów biznesowych (zainteresowanych stron), wykorzystując do tego celu np. funkcję rzecznika prasowego, który umiejętnie przekaże informacje o ewentualnym incydencie, eksponując podjęte działania sterujące[49].

Kolejne założenie budujące przestrzeń paradygmatu prawo – technicznego związane jest z postrzeganiem zachowania bezpieczeństwa informacji przez pryzmat ich „poufności", co w przypadku zabezpieczania danych osobowych pacjentów jest założeniem błędnym. Konieczność stosowania zabezpieczeń realizujących dodatkowo „dostępność" i „integralność" wynika m.in. z prawa pacjenta do informacji, dokumentacji medycznej i prawa do udzielania zgody na realizację procedurach medycznych związanych z realizacją świadczenia zdrowotnego[50].

Praktyka wskazuje, iż poufność danych osobowych znajdujących się w dokumentacji medycznej papierowej, jak i elektronicznej jest zapewniana dzięki świadomości personelu dotyczącej wymagań ustawowych[51]– co stanowi w ocenie najwyższego kierownictwa wystarczający warunek zabezpieczający.

Często jednak bez odpowiednich zabezpieczeń np. w postaci oświadczeń o zachowaniu poufności lub odpowiednich klauzul w umowach o pracę lub cywilno – prawnych dopuszczani do pracy są pracownicy wykonujący zawody „niemedyczne" uczestniczący w przetwarzaniu danych osobowych pacjentów. Sygnalizowany problem posiada perspektywę, która rozciąga się miedzy innymi na pracowników firm outsourcingowych oraz firmy leasingujące placówkom ochrony zdrowia sprzęt medyczny i oprogramowanie (np. niezbędne do funkcjonowania laboratoriów analitycznych).

Można założyć, iż eliminacja wcześniej eksponowanych założeń paradygmatu prawno - technicznego jest podstawą systemowych zmian w organizacji pozwalających na uporanie się z właściwą realizacją wymagań prawnych, które w wielu przypadkach dają pewną swobodę w implementacji zabezpieczeń - jednak pozorną, co w praktyce generuje szereg problemów natury organizacyjno - ekonomicznej.

4. Zakończenie

Skuteczność i racjonalność działań związanych z nadzorowaniem danych prawnie chronionych przetwarzanych w systemach teleinformatycznych jest w dużej mierze pochodną stosowania narzędzia jakim jest wdrożony, utrzymywany i doskonalony system zarządzania, w którym skutecznie funkcjonują procedury: zarządzania ryzykiem, działań korygujących i zapobiegawczych, audytów wewnętrznych, przeglądu zarządzania, nadzorowania wyrobu niezgodnego (procedury, której specyfika może znaleźć zastosowanie w nadzorowaniu incydentów związanych z bezpieczeństwem) oraz szereg innych elementów systemowego podejścia do zarządzania[52].

Zaimplementowane do porządku prawnego przez prawodawcę narzędzia o charakterze zarządczym (funkcjonujące na płaszczyźnie zarządzania ryzykiem [53]) tworzą kompleksowy model ochrony informacji, który posiada przymiot elastyczności pozwalający na właściwą realizację ustalonych porządkiem konstytucyjnym praw i wolności człowieka kształtujących status informacyjny jednostki mimo pojawiających się nowych zagrożeń wynikających z rozwoju socjotechnicznego społeczeństwa.

Dzięki systemowemu podejściu do ochrony danych osobowych „jednostki - pacjenta" kształtująca się coraz wyraźniej perspektywa rozwoju usług medycznych on-line wpisana jest w przestrzeń wymagań prawnych dających możliwości stosowania środków zabezpieczania komplementarnych do elementów kultury organizacyjnej podmiotów zobowiązanych przy jednoczesnym zachowaniu wysokiego poziomu zabezpieczania na podstawie wymagań prawnych kształtujących jego poziom minimalny.

Czy pytania dotyczące metanoi doświadczanej przez najwyższe kierownictwo, rewizji paradygmatu techniczno – prawnego stawiane w kontekście przyjętego i doskonalonego[54] przez

[48] Mając na uwadze wymagania prawne i regulowany na ich podstawie dostęp do określonych grup informacji posiadających różny stopnień sensytywności.

[49] Działania korygujące lub zapobiegawcze związane odpowiednio z eliminacją przyczyn incydentu lub potencjalnej przyczyny incydentu.

[50] Patrz rozdział 3,5,7 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U.2009.52.417 ze zm.).

[51] Np. art. 40 ustawy o zawodzie lekarza i lekarza dentysty (Dz.U. 2002.21.204 ze zm.), art. 21 ustawy o zawodzie pielęgniarki i położnej (Dz.U. 2009.151.1217 ze zm.), art. 29 ustawy o diagnostyce laboratoryjnej (Dz.U. 2001.100.1083 ze zm.).

[52] Np. trening dyscyplin zarządzania, które P. Senge opisał w swojej książce „Piąta dyscyplina".

[53] Patrz art. 49 ust.10 ustawy o ochronie informacji niejawnej (Dz.U.2010.182.1228); § 5 ust. 2 pkt. 1 projektu Rozporządzenia ws. podstawowych wymagań bezpieczeństwa teleinformatycznego projektowanego na podstawie delegacji art. 49 ust. 1 ustawy o ochronie informacji niejawnych; załączniku nr 6 § 3 ust. 4 Rozporządzenia w sprawie w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz.U. 2011.14.67).

[54] Rzecz w planowanych zmianach np. dotyczących Systemu Informacji Medycznej.

prawodawcę modelu systemowej ochrony danych pozwolą na uzyskanie jednoznacznych odpowiedzi potwierdzających jego skuteczność?[55] Można sądzić, że tak, ale w odpowiedniej perspektywie czasowej, pozwalającej na zgromadzenie odpowiednich zasobów finansowych i ludzkich.

Należy jednak pamiętać, iż przyjęte rozwiązania międzynarodowych standardów związanych z zarządzaniem oprócz faktu, iż są elementem obowiązującego porządku prawnego są narzędziem, którego stosowanie należy ciągle doskonalić przyjmując ducha kaizen[56].

[55] W odniesieniu do ochrony danych osobowych pacjentów lub innych informacji prawnie chronionych.

[56] „Kai" - zmiana, „zen" - dobry, czyli ciągłe doskonalenie) - filozoficzne podejście do zarządzania wywodzące się z japońskiej kultury i praktyki zarządzania. Filarem tego nurtu filozoficznego w zarządzaniu jest założenie, że jakość sprowadza się do stylu życia - niekończącego się procesu ulepszania realizowanego w oparciu o włączenie procesu myślowego na każdym etapie produkcji, Założenie to jest odpowiedzią na zautomatyzowane tradycyjne podejście do produkcji masowej, które eliminuje potrzebę świadomej oceny wykonywanego zadania. Kwestie zarządzania zasobami niezbędnymi do realizacji przyjętego modelu zarządzania ochroną informacji (mając na uwadze realia ekonomiczne) należy w ocenie autora opracowania podporządkować trzem z 10 głównych zasad kaizen: „Wymówki, że czegoś się nie da zrobić, są zbędne.", „Wybieraj proste rozwiązania, nie czekając na te idealne.", „Użyj sprytu zamiast pieniędzy."