Rekomendacje Centrum Systemów Informacyjnych Ochrony Zdrowia w zakresie bezpieczeństwa oraz rozwiązań technologicznych stosowanych podczas przetwarzania dokumentacji medycznej w postaci elektronicznej

Załącznik nr 5

Chmura obliczeniowa – SaaS (Oprogramowanie jako usługa)

EZDROWIE
CENTRUM SYSTEMÓW INFORMACYJNYCH OCHRONY ZDROWIA
ul. Stanisława Dubois 5A • 00-184 Warszawa, Polska
tel: +48 22 597-09-27 • fax: +48 22 597-09-47
biuro@csioz.gov.pl • www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP

Spis treści

Chmura obliczeniowa – SaaS (Oprogramowanie jako usługa) 1
1. Wprowadzenie 4
2. Organizacja bezpieczeństwa informacji 6
2.1. Role w zakresie Polityki Bezpieczeństwa 6
2.2. Dokumentacja 8
2.3. Okresowe audyty bezpieczeństwa 11
3. Bezpieczeństwo fizyczne i środowiskowe 14
3.1. Obszary bezpieczne 14
3.2. Bezpieczeństwo sprzętu 17
4. Bezpieczeństwo sieciowe 23
5. Bezpieczeństwo systemów klasy EDM 26
5.1. Ochrona antywirusowa 27
5.2. Usługi dostarczane przez strony trzecie 28
5.3. Planowanie i odbiór systemów 28
5.4. Zarzadzanie zmianą 29
5.5. Szyfrowanie danych medycznych 30
6. Kontrola dostępu 31
6.1. Zarzadzanie tożsamością (uwierzytelnianie) 31
6.2. Zarządzanie dostępem użytkowników 31
6.3. Odpowiedzialność użytkowników 32
6.4. Kontrola dostępu do aplikacji klasy EDM 34
6.5. Kontrola dostępu do sieci 34
6.6. Praca na odległość, wykorzystywanie urządzeń przenośnych 35
7. Stosowanie podpisu elektronicznego 36
8. Audytowalność i niezaprzeczalność danych i zdarzeń w systemie 41
9. Archiwizacja danych medycznych 43
10. Zarządzanie incydentami związanymi z bezpieczeństwem informacji 45
11. Zarządzanie ciągłością działania 47

11.1. Tworzenie i odtwarzanie kopii zapasowych 48
11.2. Dostępność i niezawodność (SLA) 49
11.3. Postępowanie na wypadek awarii/katastrofy i utraty danych 50
12. Działania dodatkowe 52

1. Wprowadzenie

Niniejszy załącznik opisuje minimalne wymagania i zalecenia dotyczące bezpiecznego przetwarzania elektronicznej dokumentacji medycznej dla modelu Cloud computing (chmura obliczeniowa). Opisane poniżej zalecenia dotyczą rozwiązania typu SaaS (Oprogramowanie jako usługa), opisanego w rozdziale 3.3 dokumentu głównego: „*Rekomendacje Centrum Systemów Informacyjnych Ochrony Zdrowia w zakresie bezpieczeństwa oraz rozwiązań technologicznych stosowanych podczas przetwarzania dokumentacji medycznej w postaci elektronicznej*". Ze względu na uwarunkowania prawne przestawione w rozdziale 3.3, możliwe jest korzystanie tylko z prywatnej chmury obliczeniowej, z opisanym w rozdziale 3 zastrzeżeniem, iż Ministerstwo Zdrowia zainicjowało stosowne zmiany legislacyjne doprecyzowujące regulacje w zakresie przetwarzania elektronicznej dokumentacji medycznej.

Software as a Service – SaaS (Oprogramowanie jako usługa) to usługa, w ramach której odbiorca uzyskuje dostęp nie tylko do infrastruktury sprzętowej wraz ze środowiskiem operacyjnym, ale również do określonych aplikacji. W przypadku wyboru tego modelu firma zewnętrzna, świadcząca usługi jest odpowiedzialna za zapewnienie bezpieczeństwa zarówno na poziomie sprzętu, jak i oprogramowania.

W tym modelu placówka medyczna jest odpowiedzialna za wybór odpowiedniego dostawcy usługi SaaS, któremu powierzy dane medyczne.

Powierzenie przetwarzania danych osobowych możliwe jest wyłącznie po spełnieniu warunków i wymagań wynikających z obowiązujących przepisów prawa, w szczególności z:

- Ustawy o ochronie danych osobowych, która w art. 31 określa podstawowe wymagania dla umowy o powierzenie przetwarzania danych,
- Ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, która w rozdziale 7 określa prawa pacjenta w zakresie dostępu do dokumentacji medycznej,
- Rozporządzenie Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. 2015 poz. 2069)- określającego wymagania dla dokumentacji w formie elektronicznej.

Umowa musi gwarantować zachowanie bezpieczeństwa danych na poziomie nie niższym niż wymagany przepisami prawa, jak również nie może powodować żadnego uszczerbku w prawach pacjenta względem dokumentacji medycznej, a w szczególności nie może utrudniać mu dostępu do tej dokumentacji czy poszerzać kręgu osób uprawnionych do takiego dostępu.

Należy zwrócić również uwagę, aby umowa zawierała zapis umożliwiający placówce medycznej możliwość audytowania firmy zapewniającej usługę SaaS w zakresie zapewnienia bezpieczeństwa powierzonych danych.

Dla każdego z poniżej opisanych punktów zaznaczono po której stronie, placówki medycznej czy też firmy, w której usługa została wykupiona, leży odpowiedzialność za zapewnienie bezpieczeństwa dokumentacji medycznej.

Szczególną uwagę należy zwrócić na zagadnienia, za których bezpieczeństwo odpowiada placówka medyczna:

1. Bezpieczeństwo pomieszczeń placówki medycznej, gdzie przetwarzane są dane medyczne (rozdział 3.1).
2. Bezpieczeństwo sprzętu będące w gestii placówki medycznej (rozdział 3.2).
3. Odpowiedzialność użytkowników (rozdział 6.3).
4. Praca na odległość, wykorzystywanie urządzeń mobilnych (rozdział 6.6).
5. Stosowanie podpisu elektronicznego (rozdział 7).
6. Zarzadzanie incydentami związanymi z bezpieczeństwem informacji (rozdział 10).
7. Zarzadzanie ciągłością działania (rozdział 11).
8. Działania dodatkowe (rozdział 12).

2. Organizacja bezpieczeństwa informacji

2.1. Role w zakresie Polityki Bezpieczeństwa

Odpowiedzialność:

Placówka medyczna: Administrator danych, Administrator Bezpieczeństwa Informacji, Audytor Bezpieczeństwa, Kierownik jednostki/organizacji, Administrator lokalny, Użytkowni, Właściciel systemu, Koordynator działań kryzysowych.

Firma zapewniająca usługę PaaS: Administrator budynku, Administrator Sieci komputerowych, Audytor bezpieczeństwa, Administrator infrastruktury sprzętowej, Koordynator działań kryzysowych, Administrator Bazy danych, Administrator bezpieczeństwa systemu, Administrator Systemu

W celu zapewnienia należytej ochrony danych zawartych w dokumentacji medycznej przechowywanej przez Usługodawcę wyznacza się określone role, którym przydzielony zostaje określony zakres odpowiedzialności.

Poniższa tabela przestawia listę ról biorących udział w zapewnieniu bezpieczeństwa informacji w Organizacji wraz z zakresem odpowiedzialności.

Lp.	Rola	Zakres odpowiedzialności	Uwagi
1.	Administrator Danych (AD)	Organ, jednostka organizacyjna, pomiot lub osoba, decydująca o celach i środkach przetwarzania danych osobowych. Administrator danych jest powoływany na podstawie ustawy o ochronie danych osobowych, jest odpowiedzialny za przetwarzanie danych osobowych w systemie, wykonuje on czynności przewidziane w ww. ustawie. Administrator może powierzyć przetwarzanie danych innemu podmiotowi w drodze umowy zawartej na piśmie.	Definicja z ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997r.
2.	Administrator Bezpieczeństwa Informacji (ABI)	Osoba wyznaczona przez Administratora danych, odpowiedzialna za nadzór nad przestrzeganiem ustanowionych zasad ochrony danych. ABI powoływany jest na podstawie ustawy o ochronie danych osobowych. Rolę Administratora danych i Administratora bezpieczeństwa informacji może pełnić jedna osoba.	Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997r.

3.	Administrator Systemu	Podmiot odpowiedzialny za technicznoorganizacyjną obsługę systemu EDM. Osoba lub zespół odpowiedzialny za administrację systemem EDM.	
4.	Administrator Bazy danych	Osoba lub zespół odpowiedzialny za administrowanie bazami danych w ramach systemu EDM.	
5.	Administrator Sieci komputerowych	Osoba lub zespół odpowiedzialny za administrowanie/zarządzanie siecią komputerową usługodawcy.	
6.	Administrator infrastruktury sprzętowej	Osoba lub zespół odpowiedzialny za administrowanie/zarządzanie serwerami i urządzeniami bezpieczeństwa.	
7.	Administrator lokalny	Osoba lub zespół odpowiedzialny za administrowanie/zarządzanie sprzętem (komputery robocze, urządzenia mobilne) i zainstalowanym oprogramowaniem (system operacyjny, oprogramowanie antywirusowe) będącym w gestii placówki medycznej (w zależności od wybranego modelu).	
8.	Administrator budynku	Osoba lub zespół odpowiedzialny za administrowanie budynkami, w których są zainstalowane urządzenia, wykorzystywane do przetwarzania danych medycznych.	
9.	Administrator Bezpieczeństwa Systemu	Osoba lub zespół odpowiedzialny za ocenę i zarzadzanie procesem zapewnienia bezpieczeństwa systemu.	
10.	Audytor bezpieczeństwa	Osoba posiadająca kompetencje (wykazane cechy osobowości oraz wykazaną zdolność stosowania wiedzy i umiejętności) do przeprowadzenia audytu, czyli systematycznego, niezależnego i udokumentowanego procesu uzyskiwania dowodu z audytu (zapisów, stwierdzeń faktów, informacji, które są istotne z uwagi na kryteria audytu i możliwe do zweryfikowania) oraz jego obiektywnej oceny w celu określenia stopnia spełnienia kryteriów audytu, czyli polityk, procedur,	

		wymagań. Audytorem może być osoba będąca pracownikiem usługodawcy, niezależna od struktur odpowiedzialnych za bezpieczeństwo w organizacji lub instytucji zewnętrznej.	
11.	Kierownik jednostki/organizacji	Kierownik placówki medycznej, Kierownik jednostki / organizacji, w której są przetwarzane dane medyczne odpowiada za zorganizowanie i zapewnienie odpowiednich środków ochrony danych.	
12.	Użytkownik	Użytkownik systemu, osoba wykorzystująca sprzęt i oprogramowanie systemu EDM do wykonywania zadań służbowych.	
13.	Właściciel systemu	Osoba odpowiedzialna za podejmowanie decyzji w zakresie wszystkich aspektów związanych z systemem.	
14.	Koordynator Działań Kryzysowych	Osoba odpowiedzialna za kierowanie pracami zespołów kryzysowych w razie wystąpienia katastrofy.	

Tabela 1. Lista ról biorących udział w zapewnieniu bezpieczeństwa informacji w Organizacji wraz z zakresem odpowiedzialności

2.2. Dokumentacja

Odpowiedzialność: Placówka medyczna, firma zapewniająca usługę SaaS

Opisana poniżej dokumentacja powinna być opracowana zarówno przez placówkę świadcząca usługi medyczne, jak i przez firmę zewnętrzną, która dostarcza sprzęt, każda w zakresie swojej odpowiedzialności, opisanym w rozdziale 1.

Ustawodawca [1] nałożył na Administratora Danych obowiązek opracowania i wdrożenia Polityki Bezpieczeństwa oraz Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych. Administrator Danych ma obowiązek prowadzić powyższą dokumentację w postaci pisemnej.

[1] Rozporządzenie Ministra Spraw Wewnętrznych i administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych.

2.2.1. Polityka Bezpieczeństwa

Zgodnie z Rozporządzeniem[2] Polityka Bezpieczeństwa powinna zawierać w szczególności:

1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
4) sposób przepływu danych między poszczególnymi systemami;
5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Ponadto, zgodnie z normą[3] zaleca się, aby Polityka Bezpieczeństwa zawierała:

- deklarację zaangażowania Kierownictwa organizacji, potwierdzającą wprowadzane cele oraz zasady bezpieczeństwa informacji w odniesieniu do strategii;
- definicję bezpieczeństwa informacji, jego ogólne cele, zakres oraz znaczenie bezpieczeństwa, jako mechanizmu umożliwiającego współużytkowanie informacji;
- strukturę szacowania i zarzadzania ryzykiem;
- definicje ogólnych i szczegółowych obowiązków w odniesieniu do zarządzania bezpieczeństwem informacji, w tym zgłaszania incydentów związanych z bezpieczeństwem informacji;
- odsyłacze do bardziej szczegółowych polityk bezpieczeństwa, procedur poszczególnych systemów informatycznych lub zalecanych zasad bezpieczeństwa do przestrzegania przez użytkowników.

Zaleca się, aby dokument Polityki Bezpieczeństwa został zatwierdzony przez Kierownictwo organizacji. Z jego treścią powinni zapoznać się wszyscy użytkownicy systemu/pracownicy organizacji oraz osoby pochodzące z zewnątrz organizacji, których zapisy mogą dotyczyć.

[2] Rozporządzenie Ministra Spraw Wewnętrznych i administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych.

[3] PN-ISO/IEC 27002:2014-12 Technika informatyczna - Techniki bezpieczeństwa - -- Praktyczne zasady zabezpieczania informacji,.

2.2.2. Instrukcja Zarządzania Systemem Informatycznym

Instrukcja Zarządzania Systemem Informatycznym jest dokumentem eksploatacyjnym dla systemów klasy EDM. Przedstawia ona procedury i zasady administrowania oraz zarządzania systemem informatycznym przetwarzającym dane osobowe. W myśl powyższego Rozporządzenia[4] Instrukcja Zarzadzania Systemem Informatycznym powinna zawierać:

1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;
2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
5) sposób, miejsce i okres przechowywania:
    a) elektronicznych nośników informacji zawierających dane osobowe,
    b) kopii zapasowych, o których mowa w pkt 4,
6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
7) sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4, tj. *„dla każdej osoby, której dane osobowe zostały przetwarzane w systemie informatycznym – z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie – system ten powinien zapewnić odnotowanie informacji o odbiorcach danych, w rozumieniu art. 7 pkt 6 ustawy o ochronie danych osobowych[5], którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych„*;
8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych;

[4] Rozporządzenie Ministra Spraw Wewnętrznych i administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych.

[5] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 2016 nr 0 poz. 922),

9) sposób stosowania środków zapewniających poufność i integralność danych, w przypadku gdy urządzenia i nośniki zawierające dane medyczne przekazywane są poza obszar, w którym dane są przetwarzane.

Zarówno Polityka Bezpieczeństwa, jak i Instrukcja Zarzadzania Systemem Informatycznym powinny być na bieżąco przeglądane i aktualizowane. Jest to proces niezbędny w celu utrzymania właściwego poziomu polityki bezpieczeństwa danych medycznych, a także w celu zachowania przydatności, skuteczności i adekwatności dokumentów.

Zaleca się aby polityka bezpieczeństwa podlegała okresowym przeglądom w ramach audytów bezpieczeństwa.

2.3. Okresowe audyty bezpieczeństwa

Odpowiedzialność: Placówka medyczna, firma zapewniająca usługę SaaS

Odpowiedzialność za wykonywanie okresowych audytów bezpieczeństwa spoczywa zarówno na placówce świadczącej usługi medyczne jak i na firmie zewnętrznej, która dostarcza sprzęt. Istotne jest aby placówka medyczna w zawartej umowie z firmą zagwarantowała sobie zapis, dający jej prawo audytowania firmy zewnętrznej pod kątem bezpieczeństw w zakresie usług jakie zostały wykupione przez placówkę. Audyty bezpieczeństwa mogą być wykonywane przez placówkę lub zlecane podmiotowi trzeciemu, wyspecjalizowanemu w tego rodzaju działalności.

Główną metodą kontroli bezpieczeństwa systemu jest prowadzenie audytów bezpieczeństwa. Audyty mogą być prowadzone przez osobę albo komórkę wewnętrzną organizacji lub przez instytucję zewnętrzną wyspecjalizowaną w takiej działalności.

Celem przeprowadzenia audytu bezpieczeństwa jest zweryfikowanie oraz potwierdzenie zgodności zapisów Polityki Bezpieczeństwa ze stanem faktycznym, zgodności stosowania norm, procedur wskazanych w Polityce Bezpieczeństwa, dokonywanie przeglądów ryzyka. Działanie to prowadzi do ciągłego podnoszenia bezpieczeństwa przechowywanych danych. Szczegółowe cele poszczególnych audytów ustalane są indywidulanie.

Szczegółowy zakres audytu powinien być ustalony z Właścicielem systemu, a prace powinny być nadzorowane. Zaleca się aby osoby prowadzące audyt miały dostęp do danych tylko w formie odczytu. Dane medyczne pacjentów powinny być szyfrowane lub maskowane, aby uniemożliwić dostęp do nich osobom nieuprawnionym. Wszystkie czynności wykonywane podczas audytu w systemie powinny być monitorowane i logowane w systemie zdarzeń, aby ograniczyć możliwość nadużyć.

Audyty wewnętrzne

Zaleca się aby planowanie audytów wewnętrznych systemu informatycznego odbywało się w systemie półrocznym, przy czym określenie częstotliwości prowadzenia audytów powinno być powiązane z analiza ryzyka. Za wykonanie planu odpowiedzialny jest Administrator Bezpieczeństwa Informacji we współpracy z Kierownictwem organizacji.

Audyty wewnętrzne prowadzone są przez audytorów niezależnych, oznacza to, iż danego systemu nie może audytować audytor będący pracownikiem podległym służbowo kierownikowi audytowanej komórki organizacyjnej lub systemu. Osoby przeprowadzające audyt muszą posiadać odpowiednie umiejętności i doświadczenie. Zaleca się aby osoba wykonująca audyt wewnętrzny posiadała odpowiednie kompetencje np.: potwierdzone certyfikatem CISA (Certified Information Systems Auditor).

Przed planowanym audytem Kierownik komórki audytowanej jest informowany o audycie. Zobowiązany jest on zapewnić dostęp do zasobów kierowanej przez niego komórki w celu przeprowadzenia audytu.

Przegląd systemu powinien obejmować zgodność z wdrażaną Polityka Bezpieczeństwa. Obszary, jakie należy wziąć pod uwagę podczas kontroli infrastruktury teleinformatycznej to:

- Infrastruktura sieciowa (switche, routery), architektura sieci, reguły dostępu;
- Systemy operacyjne na serwerach;
- Systemy zabezpieczeń sieciowych (firewalle, systemy IPS);
- Bazy danych;
- Autoryzacja oraz nadawanie uprawnień w systemach;
- System antywirusowy;
- System tworzenia kopii zapasowych i archiwizacji;
- Logowanie zdarzeń;
- System poczty elektronicznej;
- Serwis internetowy;
- Bezpieczeństwo fizyczne i środowiskowe (Bezpieczeństwo sprzętu, obszary bezpieczne);
- Wykorzystywane mechanizmy kryptograficzne.

Prowadzący audyt jest zobowiązany do przygotowania dokumentacji związanej z audytem, tj. protokołów, kart spostrzeżeń, niezgodności, raportu końcowego z audytu wraz z zaleceniami poaudytowymi.

Poza audytami planowymi mogą zostać przeprowadzone również audyty pozaplanowe, organizowane przez Kierownika organizacji. Audyty pozaplanowe z reguły realizowane są w przypadku wystąpienia incydentu naruszenia bezpieczeństwa lub na zlecenie, w miarę aktualnych potrzeb.

Zadania związane z prowadzeniem audytu można powierzyć podmiotowi zewnętrznemu, o czym mowa w poniższym akapicie.

Audyty zewnętrzne

Poza prowadzeniem audytów wewnętrznych zaleca się korzystanie z zewnętrznych audytów bezpieczeństwa systemu. Audyty zewnętrzne powinny być prowadzone przez firmy/instytucje mające wiedzę i doświadczenie w przeprowadzaniu tego typu przeglądów. Podmioty te, w ramach oferty, powinny przedstawić informacje na temat składu zespołu audytorskiego, w tym doświadczenie, kwalifikacje oraz posiadane certyfikaty w zakresie bezpieczeństwa. Zaleca się aby osoba przeprowadzająca audyt bezpieczeństwa posiadała certyfikat CISA (Certified Information Systems Auditor), natomiast inni członkowi zespołu audytującego posiadali certyfikaty potwierdzające kompetencje z obszaru bezpieczeństwa IT, np.:

• CISSP (Certified Information Systems Security Professional);

• CISM (Certified Information Security Manager), lub równoważne.

Wykonanie audytu powinno poprzedzać zawarcie umowy z podmiotem audytującym. Umowa powinna zawierać postanowienia zapewniające zachowanie bezpieczeństwa danych pozyskanych przez audytorów, określać warunki audytu oraz czas, w jakim audyt ma być przeprowadzony.

Kierownik organizacji informuje właściciela systemu o terminie i zakresie planowanego audytu zewnętrznego.

Audytor zewnętrzny prowadzi audyt zgodnie z obowiązującymi przepisami prawa oraz normami. Na bieżąco przygotowuje również dokumentację w postaci raportów i analiz.

Audyt zewnętrzny, podobnie jak audyt wewnętrzny powinien być prowadzony m.in. w następujących obszarach:

- Infrastruktura sieciowa (switche, routery), architektura sieci, reguły dostępu;
- Systemy operacyjne na serwerach;
- Systemy zabezpieczeń sieciowych (firewalle, systemy IPS);
- Bazy danych;
- Autoryzacja oraz nadawanie uprawnień w systemach;
- System antywirusowy;
- System tworzenia kopii zapasowych i archiwizacji,;
- Logowanie zdarzeń;
- System poczty elektronicznej;
- Serwis internetowy;
- Bezpieczeństwo fizyczne i środowiskowe (Bezpieczeństwo sprzętu, obszary bezpieczne);
- Wykorzystywane mechanizmy kryptograficzne.

Zaleca się korzystanie z audytów zewnętrznych raz w roku, przy czym ostateczne określenie częstotliwości prowadzenia audytów powinno być powiązane z analizą ryzyka.

Wyniki audytów zarówno wewnętrznych, jak i zewnętrznych powinny być przeanalizowane przez Kierownictwo. W razie potrzeby wdrożone powinny być odpowiednie działania naprawcze i korygujące, mające na celu usunięcie zidentyfikowanych nieprawidłowości.

3. Bezpieczeństwo fizyczne i środowiskowe

Niezależnie od przyjętego modelu przechowywania elektronicznej dokumentacji medycznej należy zadbać o zapewnienie najwyższego poziomu bezpieczeństwa przechowywanych danych. Należy zapewnić właściwy poziom ochrony zasobów, dostosowany do potencjalnych zagrożeń, zidentyfikowanych na etapie szacowania ryzyka. Aby zapewnić należyty poziom bezpieczeństwa należy dokonać separacji systemu na oddzielne segmenty w płaszczyźnie fizycznej i logicznej. Niniejszy rozdział opisuje najważniejsze założenia dotyczące bezpieczeństwa w warstwie fizycznej.

3.1. Obszary bezpieczne

Odpowiedzialność:

- **w zakresie zapewnienia bezpieczeństwa w obszarach o podwyższonym poziomie bezpieczeństwa, w tym ogólnodostępnych –** Placówka medyczna;
- **w zakresie zapewnienia bezpieczeństwa w obszarach krytycznych –** firma zapewniająca usługę SaaS.

Aby bezpiecznie przechowywać dane należy wziąć pod uwagę zarówno miejsce ich wprowadzania, jak i przechowywania. Konieczność wskazania miejsc przechowywania danych wynika z Rozporządzenia[6].

1. Zgodnie z prawem w opracowanej Polityce bezpieczeństwa należy określić wykaz budynków, pomieszczeń, w których będą przetwarzane dane osobowe.
2. Należy przeprowadzić analizę mającą na celu wyznaczenie pomieszczeń i stref bezpieczeństwa, uwzględniającą m.in. rozmiar pomieszczenia, rodzaj przechowywanych danych, czynniki środowiskowe lokalizacji, możliwość zapewnienia odpowiedniego poziomu bezpieczeństwa.
3. W ramach separacji należy wydzielić tzw. Bezpieczne strefy, tj. obszary, wśród których będą pomieszczenia o znaczeniu krytycznym oraz o podwyższonym poziomie bezpieczeństwa. Należy zidentyfikować miejsca dostępne dla użytkowników systemu, w których dane będą wprowadzane, tworzone. Strefy bezpieczeństwa wydzielane są na wniosek Właściciela

[6] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji 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 (Dz.U. 2004 r. Nr 100 poz. 1024),

systemu. Podział na strefy bezpieczeństwa, w zależności od potrzeb może wyglądać następująco:

- Pomieszczenia o podwyższonym poziomie bezpieczeństwa: pomieszczenia gdzie są wprowadzane/tworzone dane: Rejestracja, Recepcja, Izba przyjęć, gabinet lekarski, pracownia diagnostyczna, laboratorium,
- Pomieszczenia o znaczeniu krytycznym: pomieszczenia, w których będzie się znajdowała infrastruktura sieciowa, serwerowa oraz pomieszczenie Administratora Systemu.

4. Strefy bezpieczne muszą być od siebie oddzielone fizycznie.
5. Dostęp do stref bezpieczeństwa powinien być fizycznie chroniony przed dostępem osób nieuprawnionych. W szczególności konieczne jest zabezpieczenie obszarów, w których są przetwarzane dane medyczne przed dostępem osób nieuprawnionych, na czas nieobecności w nim osób upoważnionych do przetwarzania danych.
6. Przebywanie osób nieuprawnionych w obszarach, gdzie przetwarzane są dane medyczne jest możliwy wyłącznie za zgodą Administratora danych i w obecności osoby upoważnionej do przetwarzania danych osobowych, w tym danych medycznych.
7. Umieszczenie zasobów w określonych strefach możliwe jest jedynie po uprzednim wdrożeniu odpowiednich zabezpieczeń fizycznych.

Obszar bezpieczeństwa o znaczeniu krytycznym jak np. serwerownia musi:

1. Być wyposażony w system kontroli dostępu, uniemożliwiający dostęp osobom nieuprawnionym (solidnej konstrukcji drzwi, bramki, ochrona);
2. Posiadać wydajną klimatyzację;
3. Posiadać instalację przeciwpożarową w postaci wewnętrznego systemu gaszenia wraz z systemem alarmowym;
4. Posiadać zabezpieczenie przed utratą zasilania;
5. Nie posiadać otworów okiennych;
6. Posiadać pomiar parametrów takich jak: wilgotność, temperatura, które mogą w negatywny sposób wpłynąć na działanie urządzeń;
7. Posiadać monitoring wizyjny;
8. Posiadać kontrolę dostępu w postaci przynajmniej jednego z zabezpieczeń: karta dostępowa z czytnikiem elektronicznym, przepustka;
9. Być umieszczona w miejscu o minimalnym ryzyku zalania;
10. Być umieszczona w bezpiecznej odległości od materiałów łatwopalnych, grożących wybuchem;

11. Być wyposażona w instalację odgromową, należy tez stosować filtry odgromowe na liniach zasilających i komunikacyjnych.

Ponadto:

12. Obszar, na którym znajdują się krytyczne strefy bezpieczeństwa musi być monitorowany z zewnątrz.
13. Należy wziąć pod uwagę zagrożenia wynikające z otoczenia, np. zagrożenie pożarowe, przeciekającą przez dach wodę oraz zastosować środki bezpieczeństwa adekwatne do potencjalnych zagrożeń (umieszczenie sprzętu gaśniczego, odpowiednie rozmieszczenie sprzętu zapasowego i nośników danych, aby zminimalizować ryzyko uszkodzenia w momencie wystąpienia katastrofy).

Przebywanie w pomieszczeniach o znaczeniu krytycznym:

1. Musi podlegać autoryzacji;
2. Jest dozwolone wyłącznie dla osób upoważnionych lub posiadających zezwolenia wydane przez Kierownika jednostki/organizacji;
3. Jest możliwe wyłącznie w celu wykonywania obowiązków służbowych;
4. Należy zachować szczególna ostrożność, utrzymywać porządek, zamykać za sobą drzwi, nie należy podłączać urządzeń mogących spowodować zakłócenia zasilania, nie należy podłączać urządzeń mogących mieć negatywny wpływ na dyski magnetyczne oraz sprzęt;
5. Nie należy wykonywać innych czynności, które mogłyby spowodować zagrożenie dla urządzeń lub przechowywanych danych, np.: palenia, spożywania posiłków, picia napojów, nie należy zostawiać pozostałości po montażu urządzeń (np.: kartony, kable, śrubki, itd.).

Obszary o podwyższonym poziomie bezpieczeństwa typu: gabinet lekarski, laboratorium, powinny spełniać następujące wymagania:

1. Posiadać izolację fizyczną w postaci bezpiecznych drzwi;
2. Posiadać kontrolę dostępu w postaci przynajmniej jednego z zabezpieczeń: karta dostępowa z czytnikiem elektronicznym, przepustka;
3. Posiadać instalację przeciwpożarową;
4. Posiadać monitoring wizyjny drzwi wejściowych;
5. Zaleca się stosowanie monitoringu zdarzeń, systemu wykrywania włamań;
6. Zaleca się stosowanie zabezpieczeń, np. krat w oknach.

Przebywanie w pomieszczeniach o podwyższonym poziomie bezpieczeństwa:

1. Należy zachować porządek, nie pozostawiać dokumentów bez nadzoru;
2. Nie należy korzystać z urządzeń, które mogłyby zakłócić pracę sprzętu komputerowego (np.: urządzenia mogące emitować duże ilości promieniowania elektromagnetycznego, np.: nadajnik radiowy, pobierające duże ilości prądu (w sposób skokowy), podłączanie urządzeń typu wiertarka, szlifierka, itd.);
3. Należy zwracać uwagę na wszelkie zdarzenia, które mogłoby stanowić zagrożenie dla systemu i danych medycznych.

Zasady bezpieczeństwa w zakresie pomieszczeń o podwyższonym poziomie bezpieczeństwa - ogólnodostępnych, w których są przetwarzane dane osobowe, w tym dane medyczne jak np. rejestracja, recepcja.

1. Należy zachować szczególną ostrożność podczas wykonywania czynności służbowych w miejscach ogólnie dostępnych;
2. Należy stosować zapisy procedur dotyczące czystego biurka i czystego ekranu;
3. Niedopuszczalne jest opuszczenie miejsca pracy i pozostawienie go bez nadzoru;
4. Zaleca się, aby pomieszczenia, w których przetwarzane są dane miały fizyczne zabezpieczenia wejścia, do których dostęp mają tylko osoby uprawnione;
5. Regularne przeglądanie praw dostępu do pomieszczeń oraz jeśli zachodzi taka potrzeba dokonywanie aktualizacji;
6. Ślad audytowy związany z dostępem do pomieszczeń należy przechowywać w bezpieczny sposób;
7. Należy przeszkolić personel w zakresie zasad bezpieczeństwa obowiązujących na terenie placówki.

3.2. Bezpieczeństwo sprzętu

Odpowiedzialność:

- **w zakresie bezpieczeństwa sprzętu odpowiedzialność za urządzenia serwerowe i sieciowe -** firma zapewniająca usługę Hosting/SaaS;
- **w zakresie zapewnienia bezpieczeństwa sprzętu znajdującego się po stronie placówki medycznej, czyli stacji roboczych, urządzeń mobilnych -** Placówka medyczna.

Ochrona sprzętu jest niezbędna do należytego zabezpieczenia danych i systemów przed nieuprawnionym dostępem, utratą bądź modyfikacją. Należy chronić sprzęt przed zagrożeniami fizycznymi i środowiskowymi. Ochrona dotyczy również sprzętu wykorzystywanego poza siedzibą

placówki oraz wnoszonego na teren placówki. W związku z tym należy wdrożyć stosowne procedury w zakresie:

- Lokalizacji sprzętu;
- Systemów wspomagających;
- Zabezpieczenia okablowania;
- Konserwacji sprzętu;
- Bezpieczeństwa sprzętu poza siedzibą;
- Zbywania sprzętu;
- Wynoszenia sprzętu poza siedzibę.

Poniżej podano ogólne wytyczne, dotyczące zakresu informacji, który powinien się znaleźć w poszczególnych procedurach:

3.2.1. Lokalizacja sprzętu

Odpowiedzialność: Placówka medyczna, firma zapewniająca usługę SaaS, każdy w swoim zakresie:

- **lokalizacja urządzeń serwerowych i sieciowych** - firma zapewniająca usługę SaaS;
- **lokalizacja sprzętu znajdującego się po stronie placówki medycznej, czyli stacji roboczych, urządzeń mobilnych -** Placówka medyczna)

1. Sprzęt (zarówno serwery, urządzenia sieciowe, jak i komputery robocze) powinny być tak zlokalizowane, aby zminimalizować ryzyko dostępu do sprzętu osób niepowołanych, a także ograniczyć ewentualny wpływ czynników środowiskowych (np.: pożar, zalanie, dym, drgania).
2. Ponadto pomieszczenia, w których znajdują się serwery, powinny spełniać warunki opisane w punkcie 3.1.

3.2.2. Systemy wspomagające

Odpowiedzialność: Firma zapewniająca usługę SaaS

1. Zaleca się aby systemy wspomagające typu: zasilanie, klimatyzacja, oświetlenie, zaopatrzenie w wodę, itd., były dostosowane do potrzeb systemów, które obsługują.
2. Należy regularnie kontrolować poprawność funkcjonowania systemów wspomagających.
3. Dla zachowania ciągłości działania należy zapewnić więcej niż jedno źródło zasilania (dodatkowe niezależne przyłącze energetyczne, generator prądotwórczy).
4. Dla zachowania ciągłości działania elementów krytycznych (serwery, urządzenia sieciowe) należy zapewnić zasilanie gwarantowane (urządzenia UPS, agregaty prądotwórcze).

5. Należy regularnie testować sprawność działania UPS-ów, generatorów prądotwórczych.

3.2.3. Bezpieczeństwo okablowania

Odpowiedzialność: Placówka medyczna, firma zapewniająca usługę SaaS, każdy w swoim zakresie:

- **w zakresie okablowania znajdującego się w serwerowni – firma zapewniająca usługę SaaS,**
- **w zakresie okablowania pomieszczeń placówki medycznej – Placówka medyczna).**

1. Okablowanie zasilające lub telekomunikacyjne biorące udział w przesyłaniu danych należy chronić przed przepięciami oraz uszkodzeniem.
2. Zaleca się używanie jednoznacznego oznaczenia okablowania oraz sprzętu w celu uniknięcia błędów w podłączeniu.
3. Należy prowadzić dokumentację połączeń.
4. Zaleca się korzystanie z kabli światłowodowych, ekranów elektromagnetycznych do ochrony kabli, prowadzenie regularnych przeglądów okablowania pod kątem podłączonych oraz nieautoryzowanych urządzeń.

3.2.4. Konserwacja sprzętu

Odpowiedzialność: Placówka medyczna, firma zapewniająca usługę SaaS, każdy w swoim zakresie:

- konserwacji urządzeń serwerowych i sieciowych - firma zapewniająca usługę SaaS;

- konserwacji sprzętu znajdującego się po stronie placówki medycznej, czyli stacji roboczych, urządzeń mobilnych - Placówka medyczna.

1. Wykorzystywany sprzęt powinien być regularnie poddawany konserwacji. Naprawa i konserwacja sprzętu może być wykonywana wyłącznie przez osoby uprawnione.
2. Konserwacja i naprawa sprzętu powinny przebiegać zgodnie z zaleceniami producenta sprzętu.
3. Naprawa i konserwacja sprzętu poza placówką powinna być realizowana jedynie przez dział serwisu z zachowaniem szczególnej ostrożności:
    a. Należy stosować procedurę określająca zasady wynoszenia sprzętu i nośników poza siedzibę organizacji, do której zalecenia opisano w punkcie 3.2.8.;
    b. Przed przekazaniem do naprawy sprzętu wymagane jest podpisanie stosownych dokumentów uprawniających do wyniesienia sprzętu poza siedzibę oraz protokół zdawczo odbiorczy, zawierający informacje nt. jaki sprzęt został wyniesiony, osób odpowiedzialnych;

c. W przypadku gdy naprawa sprzętu nie wymaga obecności nośnika danych (dysku twardego) wszystkie nośniki należy wymontować przed przekazaniem do naprawy;

d. W przypadku gdy nie jest możliwe wymontowanie nośnika danych, należy wcześniej usunąć z niego wszelkie dane osobowe, medyczne w sposób uniemożliwiający ich odzyskanie lub przy naprawie sprzętu powinna uczestniczyć osoba uprawniona ze strony jednostki medycznej;

e. Przekazywanie do naprawy sprzętu zawierającego dane osobowe w tym dane medyczne możliwe jest wyłącznie po podpisaniu stosownej umowy z wyspecjalizowaną firmą.

3.2.5. Obsługa nośników

Odpowiedzialność: Placówka medyczna, firma zapewniająca usługę SaaS, każdy w swoim zakresie - obsługi wykorzystywanych nośników.

1. Należy wdrożyć procedurę określającą zasady postępowania w przypadku wykorzystania nośników danych zawierających dane osobowe, w tym dane medyczne.
2. Procedura powinna zawierać w szczególności następujące wytyczne:

   a. Niedozwolone jest podłączanie do komputerów nośników danych (pen drive, płyty CD/DVD, telefony komórkowe, itd. z wyjątkiem nośników niezbędnych do wykonania prac administracyjnych przez uprawnionych Administratorów;

   b. Nośniki danych w postaci dysków twardych powinny być przechowywane w odpowiednich warunkach środowiskowych, gwarantujących ich trwałość;

   c. Dyski twarde zawierające dane osobowe powinny być przechowywane w miejscach uniemożliwiających dostęp osób nieuprawnionych, w szczególności powinny być zabezpieczone fizycznie na poziomie serwerowni;

   d. W przypadku gdy nośniki (np. dyski) zawierają dane medyczne konieczne jest ich szyfrowanie. Zaleca się wykorzystanie algorytmu szyfrowania AES-256;

   e. Wszystkie nośniki danych (w tym nośniki danych zawierające kopie zapasowe) powinny być okresowo testowane;

   f. Niedopuszczalne jest kopiowanie danych osobowych, w tym danych medycznych na komputery przenośne, telefony komórkowe, itd. inne niż zatwierdzone przez Administratora Bezpieczeństwa, dopuszczone do użytku w placówce;

   g. Niedopuszczalne jest wyrzucanie nośników danych do kosza. W szczególności należy stosować procedurę dotyczącą niszczenia sprzętu i nośników danych, do której wytyczne znajdują się w punkcie 3.2.7.

3. Kierownictwo organizacji podejmuje działania mające na celu utrzymanie świadomości użytkowników w zakresie ochrony danych osobowych, w szczególności danych medycznych przechowywanych na nośnikach.

3.2.6. Bezpieczeństwo sprzętu poza siedzibą

Odpowiedzialność: Placówka medyczna

1. Zaleca się aby wykorzystanie sprzętu, na którym mogą być przetwarzane dane osobowe poza siedzibą, było autoryzowane przez Kierownictwo organizacji.
2. W celu ochrony sprzętu i danych należy wprowadzić następujące wytyczne:
    a. Zabrania się pozostawiania sprzętu w miejscach publicznych bez nadzoru;
    b. Należy stosować odpowiednie zabezpieczenia, zmniejszające ryzyko dostępu do danych osób nieuprawnionych.

3.2.7. Bezpieczna likwidacja sprzętu

Odpowiedzialność: Placówka medyczna, firma zapewniająca usługę SaaS, każdy w swoim zakresie:

- **likwidacja urządzeń serwerowych i sieciowych** - firma zapewniająca usługę SaaS;
- **likwidacja sprzętu znajdującego się po stronie placówki medycznej, czyli stacji roboczych, urządzeń mobilnych** - Placówka medyczna.

1. Decyzję o niszczeniu (brakowaniu) sprzętu lub nośników podejmuje Właściciel systemu.
2. Likwidacją sprzętu zajmuje się uprawniona do tego komórka lub firma zewnętrzna. W przypadku firmy zewnętrznej konieczne jest podpisanie stosownej umowy.
3. Sprzęt oraz wszystkie składniki sprzętu, w tym nośniki danych, powinny być niszczone w sposób bezpieczny.
4. Niedozwolone jest wyrzucanie sprzętu i nośników danych do kosza na śmieci.
5. Przed przekazaniem sprzętu do niszczenia konieczne jest trwałe, uniemożliwiające odzyskanie, usunięcie z nich danych, a gdy nie jest to możliwe uszkodzenie w sposób uniemożliwiający odczytanie danych. Samo wykasowanie danych z dysku, przed oddaniem go do utylizacji, nie powoduje trwałego usunięcia danych.
6. Trwałe usuwanie danych może odbywać się poprzez wykorzystanie specjalistycznego oprogramowania do trwałego usuwania danych. Zaleca się zastosowanie jednego z istniejących standardów oraz algorytmów dotyczących bezpiecznego usuwania danych:
    - VSITR,
    - DoD 5250.22-M,

- NAVSO P-5239-26 (MFM),
- NAVSO P-5239-26 (RLL),
- GOST P50739-95,
- algorytm Bruce'a Schneiera,
- algorytm Petera Gutmanna.

7. Niszczenie nośników danych zawierających dane medyczne powinno odbywać się poprzez ich fizyczne zniszczenie, uniemożliwiające odczytanie danych. Niszczenie dysków twardych może odbywać się np.: poprzez fizyczne niszczenie talerzy dysku, połamanie, zmielenie lub pocięcie nośników danych typu CD/DVD/biblioteki taśmowe.
8. Zalecane jest również niszczenie nośników danych poprzez zastosowanie metody termicznej albo chemicznej, powodującej zamianę dysków w ciecz, bez możliwość przywrócenia struktur nośnika.
9. Niszczenie nośników zawierających dane powinno odbywać się w obecności osób wyznaczonych przez Kierownika organizacji do pełnienia takich funkcji.
10. Niszczenie sprzętu i nośników powinno być odnotowane, należy też sporządzić protokół ze zniszczenia.
11. W przypadku gdy jakiś element sprzętu nadaje się do ponownego wykorzystania, należy go wymontować. Należy również sporządzić listę elementów do ponownego wykorzystania i przekazać ja właściwej jednostce funkcjonującej w organizacji.
12. Możliwe jest również korzystanie z usług wyspecjalizowanych firm, oferujących usługi brakowania nośników danych. W tym przypadku należy pamiętać jednak, aby:
    a. Nośniki przeznaczone do likwidacji były pozbawione zapisu danych, a w przypadku gdy nie jest to możliwe uszkodzone w sposób uniemożliwiający ich odczytanie;
    b. Niszczenie odbywało się w obecności upoważnionego pracownika organizacji;
    c. Sporządzić protokół ze zniszczenia.

3.2.8. Wynoszenie sprzętu poza siedzibę organizacji

Odpowiedzialność: Placówka medyczna

1. Należy wprowadzić procedurę regulującą wynoszenie sprzętu i nośników poza siedzibę organizacji.
2. Procedura powinna uwzględniać co najmniej następujące aspekty:

a. Sprzęt i nośniki danych nie mogą być wynoszone poza siedzibę organizacji bez specjalnego zezwolenia. Zezwolenie jest wystawiane przez osobę upoważnioną i otrzymuje je osoba wynosząca sprzęt. Procedura powinna określać listę osób upoważnionych do wystawienia zezwolenia;

b. Należy prowadzić rejestr sprzętu wynoszonego poza siedzibę. Rejestrować należy również informacje kiedy sprzęt jest zwracany;

c. Sprzęt, który zawiera dane osobowe, w tym dane medyczne, powinien być zabezpieczony poprzez szyfrowanie danych;

d. Komputery przenośne powinny:

i. Posiadać system operacyjny wymagający autoryzacji przy logowaniu;

ii. Posiadać szyfrowanie całego dysku;

iii. Posiadać aktualne oprogramowanie antywirusowe.

4. Bezpieczeństwo sieciowe

Odpowiedzialność: Placówka medyczna, firma zapewniająca usługę SaaS, każdy w swoim zakresie:

- **bezpieczeństwo sieci w zakresie zewnętrznego Data Center** - firma zapewniająca usługę SaaS;
- **bezpieczeństwo sieci lokalnej oraz sieci bezprzewodowych placówki medycznej** - Placówka medyczna)**.**

Bezpieczeństwo sieci oraz usług sieciowych jest jednym z podstawowych elementów gwarantujących bezpieczeństwo systemu EDM, danych medycznych przetwarzanych w systemie oraz wymienianych z innymi zewnętrznymi systemami np. platformą P1. Zgodnie z normą PN-ISO/IEC 17799:2007 w celu ochrony przed zagrożeniami oraz utrzymaniem bezpieczeństwa systemów, zaleca się aby administratorzy sieci wdrożyli zabezpieczenia informacji w sieciach oraz mechanizmy ochrony usług sieciowych przed nieautoryzowanym dostępem, w szczególności zaleca się:

- Rozdzielenie odpowiedzialności za działanie sieci od odpowiedzialności za działanie komputerów;
- Ustanowienie procedur i odpowiedzialności w zakresie zdalnego zarządzania sprzętem;
- Wdrożenie specjalnych zabezpieczeń w celu ochrony integralności oraz poufności danych przesyłanych przez sieci publiczne lub bezprzewodowe oraz ochrony przyłączonych systemów i aplikacji;
- Stosowanie odpowiednich mechanizmów monitorowania i tworzenia dzienników zdarzeń w celu umożliwienia rejestracji działań związanych z bezpieczeństwem;

- Koordynację działań zarządczych, aby optymalizować usługi dla organizacji oraz zapewnić, że zabezpieczenia są konsekwentnie stosowane w infrastrukturze przetwarzania informacji.

Spełnienie powyższych wytycznych wymaga realizacji wielu aspektów technicznych oraz organizacyjnych dotyczących bezpieczeństwa sieci na poziomie warstwy fizycznej oraz logicznej.

1) Bezpieczeństwo warstwy fizycznej:

   - Architektura sieci powinna zapewnić wydzielenie odpowiednich stref dostosowanych do aplikacji i usług uruchomionych w danej strefie. Strefy powinny zostać wydzielone z wykorzystaniem urządzeń firewall oraz routerów. Zaleca się aby zostały wydzielone co najmniej następujące strefy:
     - DMZ (Demilitarized Zone) - jest to ograniczona strefa zaufania, w której umieszczone są serwery dostarczające usługi dla zewnętrznych użytkowników (np. serwer WWW). Serwery w tej strefie nie posiadają dostępu do sieci wewnętrznej, w której uruchomiony jest system EDM;
     - Strefa chroniona (Secured Zone) – jest to strefa, która jest chroniona w wysokim stopniu między innymi przez zastosowanie odpowiednich konfiguracji urządzeń firewall. Nie jest możliwy bezpośredni dostęp z sieci Internet do serwerów/aplikacji umieszczonych w tej strefie. Dostęp możliwy jest tylko i wyłącznie dla zdefiniowanych hostów oraz usług. W tej strefie działa system EDM i przetwarzane są dane medyczne.
   - Architektura sieci powinna uwzględniać wdrożenie mechanizmów kompleksowej ochrony sieci przed włamaniem. Zaleca się wykorzystanie mechanizmów ochrony:
     - IPS (Intrusion Prevention System),
     - firewall,
     - sieciowy filtr antywirusowy,
     - filtr antyspamowy,
     - filtrowanie treści.
   - Należy zapewnić ochronę fizyczną oraz logiczną zdalnych portów diagnostycznych i konfiguracyjnych;
   - Kontrola dostępu do wybranych elementów sieci powinna być dodatkowo realizowana z wykorzystaniem identyfikacji urządzeń (adresy MAC).

2) Bezpieczeństwo warstwy logicznej:

- Należy wydzielić odrębne podsieci (w warstwie 2 i 3 modelu ISO/OSI);
- Należy zapewnić kontrolę routingu danych w celu zapewnienia właściwego przepływu informacji, zgodnie ze zdefiniowaną polityką kontroli dostępu do aplikacji EDM. Routing powinien zostać zrealizowany w oparciu o weryfikację adresów źródłowych i docelowych;
- Należy stosować mechanizmy filtracji i zarządzania ruchem;
- Dostęp do zewnętrznego Data Center powinien gwarantować uwierzytelnianie oraz szyfrowanie przesyłanych danych np. poprzez wykorzystanie bezpiecznego połączenia VPN IPSec;
- System EDM powinien być umieszczony w bezpiecznej strefie (Secured Zone) z wyłączeniem niezbędnych modułów komunikacyjnych umieszczonych w strefie DMZ;
- Uwierzytelnianie użytkowników przy dostępie zdalnym powinno nastąpić z wykorzystaniem wirtualnych sieci prywatnych (VPN) i silnej metody uwierzytelnienia np. tokeny sprzętowe haseł jednorazowych OTP, certyfikat elektroniczny;
- W przypadku komunikacji za pośrednictwem sieci zewnętrznej wymagane jest zastosowanie silnych mechanizmów gwarantujących ochronę przesyłanych danych, ich integralność, poufność i niezaprzeczalność (wykorzystanie protokołów SSL 3.0 / TLS 1.2).

Zabezpieczenie usług sieciowych:

- Powinna zostać utworzona polityka dotycząca korzystania z usług sieciowych definiująca:
  - Sieci i usługi sieciowe, do których dostęp jest dozwolony;
  - Procedury autoryzacji określające, kto jest uprawniony do dostępu do sieci i usług sieciowych;
  - Nadzór kierownictwa oraz procedury ochrony dostępu do połączeń sieciowych i usług sieciowych;
  - Środki wykorzystywane do realizacji dostępu do sieci lub usług sieciowych.
- Dostęp do usług powinien być możliwy tylko dla uprawnionych użytkowników/systemów poprzez zapewnienie mechanizmów uwierzytelniania i autoryzacji;
- Szczególnej ochronie podlegają komunikaty przekazywane na zewnątrz systemu EDM (np. do P1), usługi powinny gwarantować mechanizmy autoryzacji oraz poufności przesyłanych danych (w przypadku udostępnionych usług web services proponowany mechanizm to WS-Security),

Bezpieczeństwo sieci bezprzewodowych:

Ze względu na specyfikę sieci bezprzewodowych związanych z brakiem możliwości dokładnego określenia granicy sieci (dostępność sieci WiFi) wymagane jest wdrożenie odpowiednich mechanizmów bezpieczeństwa:

- Rozdzielenie sieci bezprzewodowych od sieci wewnętrznej;
- Wykorzystanie bezpiecznych algorytmów szyfrowania i uwierzytelniania w sieci (zalecane jest wykorzystywanie przynajmniej algorytmu WPA2).

Wszystkie elementy architektury sieciowej (sprzętowe oraz programowe) powinny być regularnie aktualizowane zgodnie z wymogami dostawców lub producentów sprzętu oraz oprogramowania.

Infrastruktura sieciowa powinna być na bieżąco monitorowana oraz okresowo testowana w celu weryfikacji wymaganych parametrów transmisji danych, dostępności usług oraz wykrycia ewentualnych uszkodzeń lub pogorszenia się parametrów transmisji danych.

5. Bezpieczeństwo systemów klasy EDM

Odpowiedzialność: Firma zapewniająca usługę SaaS

1. System EDM powinien być zaprojektowany oraz wdrożony zgodnie z najlepszymi praktykami bezpieczeństwa, w zakresie technologii jaka zostanie zastosowana do jego budowy. W szczególności należy zwrócić uwagę na następujące aspekty:
    a. Wykorzystanie gotowych frameworków bezpieczeństwa np. JAAS w Javie,
    b. Zastosowanie odpowiednich mechanizmów uwierzytelniania i autoryzacji – w kontekście danych medycznych zalecane jest wykorzystanie silnych metod np. bezpieczny podpis elektroniczny,
    c. Zastosowanie odpowiednich mechanizmów bezpiecznego przechowywania danych - dostęp do danych mają tylko uprawnione osoby, dane są szyfrowane (szczegółowy opis dotyczący szyfrowania został przedstawiony w pkt. 5.5), dodatkowo mogą być anonimizowane,
    d. W przypadku korzystania z aplikacji klient - serwer, szczególnie w modelu innym niż model klasyczny, wymagane jest zabezpieczenie komunikacji np.: poprzez wykorzystanie protokołu SSL (HTTPS),
    e. Mechanizm automatycznego wylogowywania po określonym czasie nieaktywności użytkownika,
    f. Logowanie niezbędnych informacji dotyczących dostępu do danych osobowych oraz danych medycznych.

2. Zalecane jest przeprowadzenie testów bezpieczeństwa systemu EDM zgodnie z aktualnymi wytycznymi np. OWASP dla aplikacji webowych. Zaleca się aby testy były przeprowadzone przed wdrożeniem oraz okresowo podczas działania aplikacji.
3. System EDM powinien być regularnie aktualizowany, zgodnie z zaleceniami producenta oprogramowania.
4. Środowisko, w którym jest zainstalowany system EDM powinno być regularnie aktualizowane, w szczególności powinno posiadać najnowsze aktualizacje bezpieczeństwa. Dotyczy to systemów operacyjnych, serwerów WWW/aplikacyjnych, baz danych itd.).
5. System operacyjny zainstalowany na stacji klienckiej powinien być regularnie aktualizowany, zgodnie z zaleceniami producenta.
6. System EDM powinien zapewnić mechanizm backupu oraz archiwizacji danych, realizowany bezpośrednio przez EDM lub przez dedykowany moduł realizujący tę funkcjonalność.
7. System EDM należy zabezpieczyć przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu.

5.1. Ochrona antywirusowa

Odpowiedzialność: Placówka medyczna, firma zapewniająca usługę SaaS, każdy w swoim zakresie:

- **oprogramowania zainstalowanego na stacjach roboczych, urządzeniach mobilnych** - Placówka medyczna;
- **serwery, brama internetowa** - firma zapewniająca usługę SaaS.

1. Dla zapewnienia bezpieczeństwa systemu EDM oraz danych medycznych należy obligatoryjnie stosować ochronę przed kodem złośliwym zarówno na poziomie stacji klienckich, urządzeń mobilnych, jak i na poziomie serwerów. Za wybór narzędzi i oprogramowania antywirusowego odpowiada Administrator Bezpieczeństwa Systemu.
    - Ochroną antywirusową powinna być również objęta brama internetowa. Zaleca się stosowanie oprogramowania antywirusowego umożliwiającego skanowanie całego dopuszczalnego przez bramkę ruchu.
2. Zaleca się wdrożenie oprogramowania antywirusowego, które umożliwiałoby automatyczną aktualizację oraz posiadało możliwość centralnego zarządzania i raportowania. Zaleca się aby oprogramowanie to umożliwiało w szczególności:
    - Zmianę ustawień konfiguracyjnych;
    - Możliwość zdalnej instalacji przez administratora lub instalacje automatyczną w momencie podłączania się komputera do sieci;
    - Automatyczną aktualizację;
    - Wymuszenie skanowania.

3. Oprogramowanie antywirusowe musi być regularnie aktualizowane (ręcznie lub automatyczne), zgodnie z zaleceniami producenta:
   - W zakresie definicji wirusów oraz sygnatur antywirusowych okresowo, przynajmniej raz w tygodniu;
   - W zakresie oprogramowania – niezwłocznie po opublikowaniu przez producenta aktualizacji bezpieczeństwa.
4. Niezbędne jest regularne skanowanie komputerów oraz serwerów przy pomocy oprogramowania antywirusowego. Okres skanowania automatycznego określa Właściciel systemu po przeprowadzeniu analizy ryzyka.
5. Zabrania się podłączania jakichkolwiek stacji klienckich oraz serwerów bez zainstalowanego oprogramowania antywirusowego.
6. Użytkownicy zobowiązani są do natychmiastowego zgłaszania podejrzenia zainfekowania swoich stacji klienckich przez wirusa.
7. Należy przeprowadzić działania edukacyjne pracowników korzystających z systemu, celem zapoznania ich z polityką antywirusowa organizacji.

5.2. Usługi dostarczane przez strony trzecie

Odpowiedzialność: Firma zapewniająca usługi SaaS

1. W przypadku gdy usługi utrzymania, modyfikacji systemu zostaną powierzone firmie zewnętrznej należy wprowadzić proces zarządzania usługami dostarczanymi przez strony trzecie.
2. Proces ten nakłada na Właściciela systemu obowiązek określenia odpowiedzialności w zakresie realizacji usług, określenia zakresu wymagań.
3. Należy podpisać umowę ze stroną trzecią. Umowa powinna zawierać co najmniej zapisy o:
   - Zachowaniu poufności danych;
   - Stosowaniu obowiązujących w organizacji określonych procedur (udostępniania powierzonych zasobów firmom i instytucjom zewnętrznym).
4. Należy regularnie przeglądać i monitorować usługi dostarczone przez strony trzecie, aby sprawdzać ich zgodność z zapisami umowy oraz odpowiednio reagować na problemy mogące wpłynąć na bezpieczeństwo systemu.

5.3. Planowanie i odbiór systemów

Odpowiedzialność: Firma zapewniająca usługi SaaS

1. W celu minimalizacji ryzyka związanego z awarią systemu EDM zaleca się wprowadzenie monitorowania i planowania wydajności systemu.
2. Zaleca się dokonywanie okresowych przeglądów zasobów (sprzętu, zasobów sieciowych, baz danych) w celu porównania wydajności urządzeń, pojemności łączy. Informacje te są konieczne w razie planowania rozbudowy systemu.
3. Zaleca się regularny przegląd umów serwisowych z dostawcami łączy, sprzętu.

5.4. Zarzadzanie zmianą

Odpowiedzialność: Firma zapewniająca usługę SaaS

1. W celu ograniczenia ryzyka wystąpienia awarii np.: w wyniku wprowadzonej zmiany systemu EDM, zaleca się wprowadzenie procedury zarzadzania zmianami.
2. Zarzadzaniu zmianą powinny podlegać:
    a. Sprzęt,
    b. Oprogramowanie,
    c. Dokumentacja,
    d. Konfiguracja,
3. Zaleca się aby proces zarzadzania zmianą zawierał co najmniej następujące kroki:
    a. Planowanie zmiany;
    b. Określenie wpływu zmiany na bezpieczeństwo systemu EDM. Zaleca się sprawdzenie czy nie zostaną naruszone zasady integralności po wprowadzeniu zmiany;
    c. Testowanie zmiany;
    d. Zatwierdzenie zmiany przez osoby upoważnione;
    e. Wprowadzenie zmiany;
    f. Udokumentowanie wprowadzenia zmiany: aktualizacja dokumentacji, której dotyczy zmiana oraz archiwizacja aktualnej dokumentacji oraz uaktualnienie dziennika zmian;
    g. Przywrócenie poprzedniej wersji systemu w przypadku gdy wprowadzenie zmiany zakończyło się niepowodzeniem.
4. Zaleca się regularne przeglądy procesu zarzadzania zmianą/konfiguracją w celu dostosowania do aktualnych potrzeb.

5.5. Szyfrowanie danych medycznych

Dostęp do danych medycznych przechowywanych i przetwarzanych w systemie EDM powinny posiadać tylko uprawnione osoby, a dodatkowo w celu zagwarantowania odpowiedniego poziomu bezpieczeństwa dane powinny być szyfrowane. Jest to szczególnie istotne w przypadku gdy placówka medyczna decyduje się na przechowywanie dokumentacji medycznej poza swoja siedzibą.

W procesie szyfrowania danych może mieć zastosowanie tzw. certyfikat korporacyjny wystawiany przez niekwalifikowane centrum certyfikacji dla danej placówki medycznej. Certyfikat będzie wykorzystywany przez uprawnionych pracowników placówki medycznej, w celu szyfrowania/odszyfrowania danych medycznych składowanych w systemie EDM np. u zewnętrznego dostawcy. W przypadku przechowywania danych medycznych u zewnętrznego dostawcy, zaleca się dodatkowo wykorzystanie urządzeń HSM do bezpiecznego przechowywania kluczy kryptograficznych szyfrujących i deszyfrujących dane.

Certyfikat korporacyjny

Certyfikat korporacyjny bazuje na certyfikatach niekwalifikowanych, które są powszechnie stosowane przez firmy, instytucje, urzędy. Jest to element systemu tzw. Infrastruktury Klucza Publicznego (PKI) w skład którego wchodzą:

- urzędy certyfikacyjne (CA, ang. Certificate Authority), dokonują wystawiania certyfikatów;
- urzędy rejestracyjne (RA, ang. Registration Authority), dokonują weryfikacji tożsamości użytkownika oraz rejestracji;
- subskrybenci certyfikatów (użytkownicy);
- oprogramowanie i infrastruktura sprzętowa.

Podstawowe funkcje, które powinny być realizowane przez każde PKI to:

- weryfikacja i potwierdzanie tożsamości subskrybentów;
- generowanie kluczy kryptograficznych;
- wystawianie i weryfikacja certyfikatów;
- podpisywanie i szyfrowanie danych.

Możliwość stosowania certyfikatu korporacyjnego przez usługodawców została przewidziana w ustawie z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia. Zgodnie z art. 16. ust. 1 ustawy, informacja o certyfikacie korporacyjnym podlegać ma ewidencjonowaniu w nowoutworzonym Centralnym Wykazie Usługodawców.

6. Kontrola dostępu

Odpowiedzialność: Placówka medyczna, firma zapewniająca usługę SaaS (każdy w swoim zakresie zgodnie z poniższym opisem).

Podmiotom przetwarzającym dane medyczne, które posiadają własną serwerownię oraz posiadają również inne systemy dziedzinowe, będące systemami zewnętrznymi do EDM, z których będą pobierane dane medyczne zaleca się wdrożenie centralnego systemu zarzadzania dostępem. Funkcjonalności tego systemu mogą być również realizowane przez moduł systemu EDM, w takim przypadku nie ma konieczności wdrażania dwóch oddzielnych systemów.

Kontrola dostępu powinna w szczególności spełniać następujące zagadnienia:

Konieczne jest zdefiniowanie polityki dostępu do systemu EDM. Powinna ona zawierać kwestie związane z ochroną prywatności i poufności danych osobowych w tym danych medycznych pacjentów.

6.1. Zarzadzanie tożsamością (uwierzytelnianie)

Odpowiedzialność: Firma zapewniająca usługi SaaS

1. Należy wprowadzić zabezpieczenia uniemożliwiające dostęp do aplikacji lub danych bez wcześniejszego uwierzytelnienia.
2. Zaleca się wprowadzenie centralnego systemu zarządzania dostępem. Umożliwia on realizowanie funkcjonalności pojedynczego logowania do zintegrowanych systemów (Single Sign-On).
3. W przypadku wdrożenia centralnego systemu zarządzania dostępem zaleca się, aby umożliwiał on integrację zewnętrznych systemów w celu zapewnienia funkcjonalności pojedynczego logowania oraz centralnego zarządzania tożsamością użytkowników we wszystkich zintegrowanych systemach.
4. W przypadku wdrożenia centralnego systemu zarządzania dostępem zaleca się, aby udostępniał on mechanizm „workflow" umożliwiający definicję procesu oraz jego realizację w odniesieniu do zarządzania użytkownikami oraz ich uprawnieniami. Definicja procesu umożliwi między innymi akceptację poszczególnych kroków procesu przez dwie osoby (np. założenie użytkownika wymaga akceptacji bezpośredniego przełożonego oraz kierownika jednostki organizacyjnej).

6.2. Zarządzanie dostępem użytkowników

Odpowiedzialność: Firma zapewniająca usługę SaaS

1. Uprawnienia użytkowników systemu nadawane są jedynie w zakresie niezbędnym do wykonywania obowiązków służbowych. Uprawnienia powinny być nadawane w możliwie minimalnym zakresie.
2. Administrator systemu nadaje uprawnienia na podstawie wniosku zatwierdzonego przez Właściciela systemu.
3. W zależności od funkcjonalności systemu zaleca się stosowanie czasowego ograniczenia ważności kont.
4. Jeśli dostęp do przetwarzanych danych w systemie informatycznym posiadają co najmniej dwie osoby, dla każdego użytkownika systemu nadawany jest unikalny identyfikator, dzięki któremu możliwa jest jednoznaczna identyfikacja.
5. Zakazuje się wykorzystywania wcześniej nadanych identyfikatorów użytkowników, którzy utracili uprawnienia do przetwarzania danych.
6. Zaleca się wprowadzenie ról użytkowników systemu, na podstawie wymagań biznesowych. Można w ten sposób stworzyć profil dostępowy użytkownika.
7. Zabrania się stosowania kont grupowych (wielu użytkowników korzysta z jednego konta).
8. Należy okresowo weryfikować nadane uprawnienia oraz dokonywać ich modyfikacji lub cofnięcia. Przepisy normatywne dopuszczają przeprowadzenie kontroli raz na 6 (sześć) miesięcy, jednak ze względu na bezpieczeństwo danych medycznych zaleca się kontrolę co 3 (trzy) miesiące.

6.3. Odpowiedzialność użytkowników

Odpowiedzialność: Placówka medyczna, Firma zapewniająca usługę SaaS

1. Wszyscy użytkownicy powinni być przeszkoleni i poinformowani o spoczywającej na nich odpowiedzialności w zakresie kontroli dostępu oraz zabezpieczenia sprzętu, z którego korzystają.
2. **Polityka haseł**: Wszyscy użytkownicy systemu zobowiązani są do stosowania polityki haseł. W przypadku gdy do uwierzytelniania używa się hasła, musi się ono składać co najmniej z 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne. Hasło należy zmieniać co 30 dni.
3. **Polityka czystego biurka:** Należy wprowadzić Politykę czystego biurka dla dokumentów papierowych i nośników elektronicznych. W przypadku dłuższej nieobecności przy stanowisku pracy lub po jej zakończeniu pracownik jest zobowiązany do umieszczenia wszelkich dokumentów i nośników zawierających dane osobowe w bezpiecznym miejscu, np. zamykanej

szafce, w celu uniemożliwienia dostęp do nich osobom nieuprawnionym. Nie należy również zostawiać dokumentów i nośników w łatwo dostępnych miejscach, np. przy urządzeniach drukujących.

4. **Polityka czystego ekranu:** W przypadku opuszczenia stanowiska pracy pracownik jest zobowiązany do wylogowania się z aplikacji lub zablokowania dostępu do pulpitu stacji roboczej, w celu uniemożliwienia dostępu do systemu lub aplikacji osoby nieupoważnionej.
5. **Zasada rozpoczęcia i zakończenia pracy** Pracownik rozpoczynając pracę powinien zalogować się do systemu/aplikacji, na zakończenie pracy musi się wylogować z systemu.
6. Zasada korzystania z urządzeń biurowych
    a. Pracownicy korzystający z urządzeń biurowych typu kopiarka, faks, drukarka nie powinni zostawiać żadnych dokumentów w otoczeniu oraz wewnątrz urządzeń, na czas dłuższy niż jest to konieczne.
    b. Organizacja procesu drukowania na urządzeniach innych niż indywidualne drukarki (dołączone tylko do jednego stanowiska roboczego) powinna zapewniać wstrzymywanie fizycznego wydruku do momentu pojawienia się przy urządzeniu drukującym i uwierzytelnienia się (np. przez podanie hasła) osoby, która wydruk zleciła.
    c. Organizacja procesu drukowania powinna zapewniać rozliczalność tego procesu metodą ukrytego znakowania dokumentów, w sposób umożliwiający co najmniej ujawnienie daty i czasu powstania wydruku oraz identyfikatora osoby, która wydruk zleciła.
    d. Urządzenia drukujące, kopiujące, faksy powinny znajdować się w miejscu niedostępnym dla osób nieuprawnionych.

7. Zasada korzystania z nośników danych

a. Należy wdrożyć procedurę postępowania z nośnikami, przechowywania i niszczenia nośników danych.
b. Nośniki danych, płyty CD/DVD, pen drive, itd., należy przechowywać w sposób uniemożliwiający dostęp osób nieuprawnionych.
c. Nośniki, które nie będą już wykorzystywane należy niszczyć w sposób trwały. Wytyczne do procedury niszczenia opisane zostały w punkcie 3.2.7.
d. Dane, które nie podlegają przechowywaniu, powinny być utylizowane.

6.4. Kontrola dostępu do aplikacji klasy EDM

Odpowiedzialność: Firma zapewniająca usługę SaaS

W celu zwiększenia bezpieczeństwa danych przechowywanych w aplikacjach klasy EDM należy wprowadzić następujące zasady:

1. Aplikacje klasy EDM powinny być zabezpieczone przed nieuprawnionym dostępem. Dostęp do nich powinni mieć wyłącznie autoryzowani użytkownicy.
2. Należy określić zasady dostępu dla użytkowników, stosując zasadę wiedzy uzasadnionej.
3. Dostęp do aplikacji odbywa się wyłącznie na podstawie zdefiniowanej w systemie metody logowania (hasło, certyfikat elektroniczny).
4. Należy określić liczbę prób bezskutecznego logowania się do aplikacji (zaleca się 3 (trzy) takie próby).
5. Należy wprowadzić mechanizm blokowania konta użytkownika, po wyczerpaniu prób logowania.
6. Należy określić maksymalny czas przeznaczony na logowanie.
7. Należy ustalić zasadę logowania się, wykorzystując politykę haseł/certyfikatów.
8. Należy uniemożliwić przesyłanie hasła otwartym tekstem. Należy ukryć wyświetlanie wpisywanego hasła podczas logowania.
9. Należy wprowadzić mechanizm blokowania ekranu lub zamykania sesji użytkownika w przypadku okresowego braku aktywności w aplikacji.
10. Nieuprawnieni użytkownicy nie mogą mieć dostępu do danych medycznych znajdujących się w systemie.
11. Wszystkie czynności wykonywane w aplikacji przez użytkowników powinny być logowane.
12. Logowane informacje muszą być zabezpieczone przed usunięciem lub modyfikacją.
13. Aplikacja musi być na bieżąco aktualizowana.
14. Wszystkie problemy z dostępem i działaniem aplikacji powinny być zgłaszane zgodnie z obowiązującą w organizacji procedurą.

6.5. Kontrola dostępu do sieci

Odpowiedzialność: Firma zapewniająca usługę SaaS

1. Kontrola dostępu realizowana jest również na poziomie sieciowym. Pracownicy szpitala mają dostęp do aplikacji jedynie z wewnętrznej sieci LAN. Aplikacja nie jest dostępna w Internecie.
2. Zasady dostępu do sieci wewnętrznej, który jest dozwolony wyłącznie dla pracowników i osób upoważnionych, należy zdefiniować w stosownej procedurze.
3. Konfiguracja urządzeń sieciowych musi uniemożliwiać osobom nieuprawnionym dostęp do sieci wewnętrznej podmiotu.
4. Dostęp do sieci może odbywać się wyłącznie z wykorzystaniem uprawnionego do tego sprzętu, dopuszczonego do użytku przez Właściciela systemu.
5. Należy kontrolować dostęp urządzenia fizycznego poprzez weryfikację adresu MAC, a gdzie to możliwe również w oparciu o technologię 802.1x.
6. Zabrania się stosowania wszelkich działań, urządzeń mogących zakłócić pracę sieci (np.: urządzenia do podsłuchiwania ruchu sieciowego, oprogramowania zakłócającego pracę sieci, próby ataków sieciowych, itd.).
7. Zabrania się podłączania do komputerów, serwerów urządzeń umożliwiających dostęp do zewnętrznych sieci operatorów telekomunikacyjnych (sieci komórkowych).

6.6. Praca na odległość, wykorzystywanie urządzeń przenośnych

Odpowiedzialność: Placówka medyczna

W celu zapewnienia bezpieczeństwa danych przetwarzanych na urządzeniach przenośnych należy wprowadzić odpowiednie regulacje.

1. Użytkownicy mogą mieć możliwość korzystania z urządzeń przenośnych (notebook, smartphone, telefony komórkowe, itd.), które zostały dopuszczone przez Właściciela systemu. Z urządzeń przenośnych (poza notebookami) nie mogą korzystać Administratorzy.
2. Dostęp zdalny do systemu EDM jest możliwy wyłącznie poprzez wykorzystanie uwierzytelnionego połączenia VPN. Uzyskanie przez użytkownika dostępu zdalnego musi być zaakceptowane przez Właściciela systemu. Niezbędne jest również przeszkolenie użytkownika w tym zakresie.
3. Użytkownik korzystający z urządzeń przenośnych jest zobowiązany do zachowania szczególnej ostrożności, aby urządzenie nie zostało zagubione, skradzione, pozostawione bez opieki. Np. komputery przenośne zawsze powinny być wożone w bagażu podręcznym i jeśli to możliwe maskowane podczas transportu.
4. Dane znajdujące się na urządzeniu przenośnym powinny być zaszyfrowane. Zaleca się wykorzystanie algorytmu szyfrowania AES-256. Użytkownik jest zobowiązany do wykonywania kopii zapasowych informacji znajdujących się na urządzeniu. Kopie zapasowe powinny być

należycie chronione, zgodnie z procedurą dotycząca tworzenia i odtwarzania kopii zapasowych.

5. Niedozwolone jest instalowanie oprogramowania innego niż zdefiniowane przez Właściciela systemu.
6. Niedozwolone jest instalowania oprogramowania niezgodnego z warunkami licencjonowania.

7. Stosowanie podpisu elektronicznego

Odpowiedzialność: Placówka medyczna, firma zapewniająca usługi SaaS

W niniejszym rozdziale zostały opisane wymagania prawne wynikające z ustaw i rozporządzeń związanych z elektroniczną dokumentacją medyczną. Przedstawiony opis zawiera odniesienia do definicji bezpiecznego podpisu elektronicznego, Profilu Zaufanego ePUAP, sposobu ich pozyskiwania i używania. Określone zostały również wymagania co do zakresu funkcjonalnego systemów elektronicznej dokumentacji medycznej w obszarze podpisu elektronicznego.

Stosowanie podpisu elektronicznego lub Profilu Zaufanego ePUAP ma na celu zapewnienie integralności, niezaprzeczalności i autoryzacji elektronicznej dokumentacji medycznej. Podpis elektroniczny należy stosować zawsze gdy tworzona jest EDM, lub gdy wprowadzane są do niej zmiany. Każdy system wspomagający funkcjonowanie EDM musi być wyposażony w moduły odpowiedzialne za pełną obsługę podpisu elektronicznego.

Wymagania prawne dot. kwalifikowanego podpisu elektronicznego w kontekście EDM

1. Rozporządzenie Ministra zdrowia z dnia 28 marca 2013 r. w sprawie wymagań dla Systemu Informacji:
   i. Określa sposób udostępniania EDM, który zakłada zgodnie z §4 ust. 1, że sposób udostepnienia ma umożliwić identyfikację uprawnionych osób, o której mowa w art. 20a ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. Identyfikacja następuje przez zastosowanie kwalifikowanego certyfikatu podpisu elektronicznego przy zachowaniu zasad przewidzianych w ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. 2016 poz. 1579), lub profilu zaufanego ePUAP.
   ii. Definiuje proces udostępniania EDM z wykorzystaniem komunikatów (proces został szczegółowo opisany w rozdziale 4.5) zgodnie z którym §5 ust. 6 mówi, że podpisanie przez pracownika medycznego usługodawcy udostępniającego elektroniczną dokumentację medyczną komunikatu przy użyciu kwalifikowanego podpisu elektronicznego w ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. 2016 poz. 1579), albo podpisu potwierdzonego profilem zaufanym ePUAP w rozumieniu art. 3 pkt 15 ustawy z

dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;

iii. Definiuje sposób przetwarzania EDM w SIM (proces został szczegółowo opisany w rozdziale 4.5) zgodnie z którym w §8 ust. 2 mówi się o wykorzystaniu komunikatów zawierających elektroniczne dokumenty SIM podpisywanych przy użyciu kwalifikowanego podpisu elektronicznego w rozumieniu z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. 2016 poz. 1579), albo podpisu potwierdzonego profilem zaufanym ePUAP w rozumieniu art. 3 pkt 15 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

2. Ustawa z 28 kwietnia 2011 r. o informacji w ochronie zdrowia:

i. Art. 16 ustawa odnosi się do Centralnego Wykazu Usługodawców, w którym są przetwarzane dane usługodawców. W ramach Centralnego Wykazu Usługodawców do nadanego usługodawcy identyfikatora przyporządkowane są dane umożliwiające identyfikację usługodawcy, w tym dane certyfikatu. Certyfikat używany jest przez usługodawcę do:

1. przekazywanych z systemu ewidencyjno-informatycznego usługodawcy danych o udzielonych usługobiorcom świadczeniach opieki zdrowotnej;
2. korekty błędnych danych o udzielonych i planowanych świadczeniach opieki zdrowotnej;
3. danych dotyczących pracowników medycznych udzielających świadczeń opieki zdrowotnej.

ii. Art. 17 odnosi się do Centralnego Wykazu Pracowników Medycznych. W ramach Centralnego Wykazu Pracowników Medycznych, do nadanego pracownikowi medycznemu identyfikatora, są przyporządkowane dane umożliwiające identyfikację pracownika medycznego, w tym dane certyfikatu. Pracownik medyczny używa certyfikatu w celu:

1. autoryzacji elektronicznej dokumentacji medycznej;
2. uzyskania dostępu do danych umożliwiających pobranie z SIM dokumentów elektronicznych wystawionych przez innego usługodawcę oraz pobrania danych z tych dokumentów, w zakresie niezbędnym do prowadzenia diagnostyki, zapewnienia ciągłości leczenia oraz zaopatrzenia usługobiorców w produkty lecznicze i wyroby medyczne;
3. uzyskania dostępu do danych zgromadzonych w SIM umożliwiających wymianę pomiędzy usługodawcami danych zawartych w elektronicznej dokumentacji medycznej. iii. Rozporządzenie Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. 2015 poz. 2069) – w przypadku dokumentacji medycznej prowadzonej w postaci elektronicznej, zgodnie z §10 ust. 2, oznaczenie osoby udzielającej świadczeń zdrowotnych może zawierać podpis elektroniczny.

Definicje związane z podpisem elektronicznym

Podpis elektroniczny – zgodnie z art. 10 ust. 10 Rozporządzeniem parlamentu europejskiego i rady (ue) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE, oznacza dane w postaci elektronicznej, które są dołączone lub logicznie powiązane z innymi danymi w postaci elektronicznej, i które użyte są przez podpisującego jako podpis.

Zaawansowany podpis elektroniczny - podpis elektroniczny, który:

a) jest unikalnie przyporządkowany podpisującemu;
b) umożliwia ustalenie tożsamości podpisującego;
c) jest składany przy użyciu danych służących do składania podpisu elektronicznego, których podpisujący może, z dużą dozą pewności, użyć pod wyłączną swoją kontrolą; oraz
d) jest powiązany z danymi podpisanymi w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna.

Certyfikat podpisu elektronicznego - oznacza poświadczenie elektroniczne, które przyporządkowuje dane służące do walidacji podpisu elektronicznego do osoby fizycznej i potwierdza co najmniej imię i nazwisko lub pseudonim tej osoby.

Kwalifikowany certyfikat podpisu elektronicznego - oznacza certyfikat podpisu elektronicznego, który jest wydawany przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej.

Dostawca usług zaufania **-** oznacza osobę fizyczną lub prawną, która świadczy przynajmniej jedną usługę zaufania, jako kwalifikowany lub niekwalifikowany dostawca usług zaufania.

Kwalifikowany dostawca usług zaufania **-** oznacza dostawcę usług zaufania, który świadczy przynajmniej jedną kwalifikowaną usługę zaufania i któremu status kwalifikowany nadał organ nadzoru.

Podpis elektroniczny i jego skutki prawne

Szczegółowe skutki prawne stosowania podpisu elektronicznego zawiera przytaczana wcześniej ustawa o usługach zaufania oraz identyfikacji elektronicznej. Najważniejsze z nich to:

1. Podpisowi elektronicznemu nie można odmówić skutku prawnego ani dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że podpis ten ma postać elektroniczną lub, że nie spełnia wymogów dla kwalifikowanych podpisów elektronicznych.
2. Kwalifikowany podpis elektroniczny ma skutek prawny równoważny podpisowi własnoręcznemu.
3. Kwalifikowany podpis elektroniczny oparty na kwalifikowanym certyfikacie wydanym w jednym państwie członkowskim jest uznawany za kwalifikowany podpis elektroniczny we wszystkich pozostałych państwach członkowskich.

Definicje związane z Profilem Zaufanym ePUAP

Profil zaufany ePUAP – zestaw informacji identyfikujących i opisujących podmiot lub osobę będącą użytkownikiem konta na ePUAP, który został w wiarygodny sposób potwierdzony przez organ podmiotu określonego w ustawie o informatyzacji podmiotów realizujących zadania publiczne. Zawiera on:

1. imię użytkownika;
2. nazwisko użytkownika;
3. numer PESEL użytkownika;
4. identyfikator użytkownika;
5. identyfikator profilu zaufanego ePUAP;
6. czas jego potwierdzenia;
7. termin ważności;
8. adres poczty elektronicznej użytkownika;
9. określenie sposobu autoryzacji.

Podpis potwierdzony profilem zaufanym ePUAP – podpis złożony przez użytkownika konta ePUAP, do którego zostały dołączone informacje identyfikujące zawarte w profilu zaufanym ePUAP, a także:

a) jednoznacznie wskazujący profil zaufany ePUAP osoby, która wykonała podpis;

b) zawierający czas wykonania podpisu;

c) jednoznacznie identyfikujący konto ePUAP osoby, która wykonała podpis;

d) autoryzowany przez użytkownika konta ePUAP;

e) potwierdzony i chroniony podpisem systemowym ePUAP.

Podpis systemowy ePUAP – podpis cyfrowy utworzony w bezpiecznym środowisku systemu ePUAP, zapewniający integralność i autentyczność wykonania operacji przez system ePUAP;

Profil Zaufany ePUAP i jego skutki prawne

Szczegółowe skutki prawne stosowania Profilu Zaufanego ePUAP zawiera ustawa z dnia 17 lutego 2005 r. o informatyzacji podmiotów realizujących zadania publiczne. Najważniejsze z nich to:

1. Podpis potwierdzony profilem zaufanym ePUAP wywołuje skutki prawne, jeżeli został utworzony lub złożony w okresie ważności tego profilu.

2. Dane w postaci elektronicznej opatrzone podpisem potwierdzonym profilem zaufanym ePUAP są równoważne pod względem skutków prawnych dokumentowi opatrzonemu podpisem własnoręcznym, chyba że przepisy odrębne stanowią inaczej.

3. Nie można odmówić ważności i skuteczności podpisowi potwierdzonemu profilem zaufanym ePUAP tylko na tej podstawie, że istnieje w postaci elektronicznej lub zmianie uległy dane inne niż służące do potwierdzenia profilu zaufanego.

Wydawanie certyfikatu kwalifikowanego

Adresy podmiotów znaleźć można na stronie Narodowego Centrum Certyfikacji (NCCert) prowadzonego przez Narodowy Bank Polski www.nccert.pl.

Niezależnie od dostawcy procedura uzyskania certyfikatu wygląda podobnie. Należy wypełnić i złożyć w punkcie rejestracyjnym wniosek, podając w nim m.in. swoje dane osobowe. Wniosek podpisywany jest własnoręcznie przez osobę ubiegającą się o certyfikat. Pracownik punktu przyjmującego wniosek dokonuje weryfikacji danych i w przypadku stwierdzenia ich poprawności kieruje go do realizacji, polegającej na wygenerowaniu certyfikatu. Certyfikat umieszczany jest na karcie kryptograficznej i najczęściej oferowany jest razem z bezpiecznym urządzeniem do składania podpisu elektronicznego.

Centra certyfikacji są podmiotami komercyjnymi, w których wydanie certyfikatu jest usługą płatną.

Uzyskiwanie Profilu Zaufanego ePUAP

Poniżej przedstawione zostały kroki jakie należy wykonać, aby pozyskać Profil Zaufany ePUAP:

1. Założyć konta na portalu www.epuap.gov.pl;

2. Wypełnić na ePUAP i zarejestrować wniosek o zaufanie profilu i wysłać go do punktu potwierdzeń (czynności realizowane są drogą elektroniczną na platformie ePUAP). Zgodnie z regulacjami prawnymi punktami potwierdzeń są:

    a. Urzędy Skarbowe;

    b. Urzędy Wojewódzkie;

    c. Placówki Zakładu Ubezpieczeń Społecznych;

    d. Za granicą placówki konsularne;

    e. I inne podmioty, które uzyskały zgodę Ministra ds. Informatyzacji na prowadzenie punktu potwierdzeń Profilu Zaufanego ePUAP. (wykaz wszystkich, ponad 930 punktów znajduje się na portalu www.epuap.gov.pl).

3. Udać się w ciągu 14 dniu do punktu potwierdzeń, gdzie upoważniony urzędnik dokona weryfikacji danych we wniosku z danymi osoby wnioskującej o Profil Zaufany ePUAP. Jeżeli dane będą zgodne to Profil Zaufany ePUAP zostanie aktywowany na okres trzech lat. W przypadku niezgodności wniosek zostanie odrzucony.

3a. Osoby posiadające bezpieczny podpis elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu mogą dokonać potwierdzenia Profilu Zaufanego ePUAP bez konieczności odwiedzania punktu potwierdzeń, przez podpisanie wniosku o Profil Zaufany ePUAP posiadanym podpisem elektronicznym.

8. Audytowalność i niezaprzeczalność danych i zdarzeń w systemie

Odpowiedzialność: Firma zapewniająca usługi SaaS

Należy podkreślić, iż zapewnienie rozliczalności czynności wykonywanych w systemie stanowi jedną z podstawowych funkcji bezpieczeństwa. Jest ono szczególnie istotne w przypadku przetwarzania danych, które zawierają dane medyczne.

Niniejszy rozdział opisuje aspekty, jakie należy wziąć pod uwagę aby zapewnić bezpieczeństwo danych, m.in. w zakresie rozliczalności, audytowalności, niezaprzeczalności.

W celu spełnienia wymagań bezpieczeństwa elektronicznej dokumentacji medycznej system EDM powinien spełniać następujące funkcje:

1. System powinien mieć włączony mechanizm audytowania zdarzeń.
2. System EDM powinien zapewniać logowanie wszystkich informacji z działalności użytkowników ze szczególnym uwzględnieniem dostępu do danych medycznych.

   Zgodnie z Rozporządzeniem[7] „System zapewnia odnotowanie:

   a. Daty pierwszego wprowadzenia danych;
   b. Identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;
   c. Źródła danych, w przypadku zbierania danych, nie od osoby, której dotyczą;
   d. Informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy o ochronie danych osobowych, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych,

   Oraz zgodnie z § 80, pkt 4 Rozporządzenia[8] System EDM powinien zapewniać identyfikację osoby dokonującej wpisu oraz osoby udzielającej świadczeń zdrowotnych i dokonanych przez

[7] Rozporządzenie Ministra Spraw Wewnętrznych i administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakimi powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych.

[8] • Rozporządzenie Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. 2015 poz. 2069)

te osoby zmian, w szczególności dla odpowiednich rodzajów dokumentacji przyporządkowanie cech informacyjnych zgodnie z art.10 ust. 2: oznaczenie osoby udzielającej świadczeń zdrowotnych oraz kierującej na badanie konsultacyjne lub leczenie:

a. nazwisko i imię;

b. tytuł zawodowy;

c. uzyskane specjalizacje;

d. numer prawa wykonywania zawodu – w przypadku lekarza, pielęgniarki i położnej;

e. podpis elektroniczny.

3. Mechanizmy komunikacji w systemie EDM powinny zapewniać niezaprzeczalność danych i zdarzeń.

4. Zastosowane środki techniczne zapewniające audytowalność muszą umożliwiać identyfikację i rejestrację urządzeń (m.in. urządzenia sieciowe, urządzenia bezpieczeństwa, serwery), systemów i osób, które biorą udział w komunikacji.

5. W celu zapewnienia niezaprzeczalności stosuje się następujące rozwiązania:

    a. Mechanizm logowania użytkownika z wykorzystaniem dwuskładnikowego uwierzytelniania (np.: hasła jednorazowe OTP, certyfikaty elektroniczne, cecha biometryczna);

    b. Stosowanie podpisu elektronicznego lub profilu zaufanego (opisanych w rozdziale 6.);

    c. Zastosowanie wytycznych polityki bezpieczeństwa dotyczących zarzadzania kontami użytkowników w systemie EDM, tj. nadanie unikalnych identyfikatorów użytkownika, nie korzystanie ponownie z tego samego identyfikatora, w przypadku gdy nie jest on już wykorzystywany;

    d. Rejestracja wszystkich czynności wykonywanych przez użytkowników w systemie EDM (identyfikator użytkownika, wykonywane działanie, czas jego wykonywania).

6. System EDM powinien umożliwiać odtworzenie historii zmian w dokumentacji medycznej z precyzyjnym określeniem:

    a. uprawnionych osób, które dokonywały zmian;

    b. czasu wykonania zmian;

    c. zakresu wykonanych zmian.

7. System EDM powinien posiadać mechanizm zapewniający rozliczalność tworzonej dokumentacji, w szczególności powinien oznaczać czasem początkowy wpis, modyfikację, wymianę danych oraz identyfikować aktora/podmiot biorący w tym udział.
8. Sposób zapisu oraz przechowywania logów powinien gwarantować integralność i niezaprzeczalność danych oraz ich bezpieczeństwa. Należy zapewnić kontrolę dostępu do logów, a także zadbać o zabezpieczenie przed ich nieuprawnionym usunięciem, modyfikacją, zniszczeniem.
9. Dostęp do logów zapewniony jest wyłącznie dla osób uprawnionych. Zalecenia procedury dostępu do danych opisano w punkcie 6.
10. Okres przechowywania logów dotyczących konkretnych danych/zdarzeń medycznych musi być co najmniej taki jaki jest wymagany dla konkretnych danych/zdarzeń medycznych.
11. System EDM powinien umożliwiać przygotowanie raportów z systemu w celu wspomagania zapewnienia zgodności systemu z wymogami dotyczącymi okresowego audytu.
    W szczególności mogą to być następujące raporty:
    a. Raport historii zmian danego dokumentu medycznego;
    b. Kto i kiedy miał dostęp do danych.
12. Logi systemu EDM powinny być regularnie przeglądane.

9. Archiwizacja danych medycznych

Odpowiedzialność: Firma zapewniająca usługi SaaS

Ustawa [9] nakłada na usługodawców obowiązek przechowywania dokumentacji medycznej przez określony okres. Szczegółowe podstawy prawne zostały opisane w rozdziale 4.6 niniejszego dokumentu. Rozdział ten opisuje techniczne aspekty archiwizacji danych medycznych. Archiwizacja polega na przenoszeniu danych z oryginalnego nośnika na nośnik zapasowy, a następnie usunięciu z oryginał. Tak rozumianą archiwizację przeprowadza się na danych, które przez określony czas powinny być przechowywane np. zgodnie z ustawą, ale nie jest konieczny do nich stały dostęp.

W celu spełnienia wymagań ustawowych:

1. System EDM powinien posiadać moduł archiwizacji danych.
2. Archiwizacji podlega dokumentacja medyczna pacjenta.

[9] Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. 2016 nr 0 poz. 186),

[10] PN-EN ISO 10781:2015-11

3. Zaleca się aby archiwizacji podlegały również logi zdarzeń pochodzące z systemu EDM oraz logi zdarzeń systemowych.
4. Tam gdzie to możliwe archiwizowane dane powinny być niezależne od technologii, aby w przyszłości użytkownicy nie byli zależni od przestarzałych technologii[10].
5. Należy archiwizować dokumentację medyczną pacjenta zgodnie z procedurami zdefiniowanymi w ramach polityki bezpieczeństwa. Procedury powinny zawierać opis techniczny realizacji archiwizacji, wykorzystywaną technologię, zakres danych podlegających archiwizacji, sposób zabezpieczenia danych oraz mechanizmy odtwarzania zarchiwizowanych danych.
6. Dane medyczne poddawane procesowi archiwizacji muszą być zaszyfrowane. Zaleca się wykorzystanie algorytmu szyfrowania AES-256. Usługodawca musi zapewnić dostęp do zaszyfrowanych danych przez wymagany okres czasu.
7. Archiwizacja powinna być wykonana na zewnętrzny nośnik danych, przechowywany w warunkach zgodnych z procedurą archiwizacji i procedurą postępowania z nośnikami danych.
8. Dostęp do zarchiwizowanej elektronicznej dokumentacji medycznej musi być zabezpieczony przez dostępem osób nieuprawnionych, zniszczeniem, modyfikacją, uszkodzeniem.
9. Zaleca się aby archiwizacja była wykonywana z użyciem nośników tylko do odczytu, aby niemożliwa była modyfikacja zapisanych danych.
10. Do najpopularniejszych nośników danych, wykorzystywanych do archiwizacji danych należą taśmy magnetyczne. Jednak nie zapewniają one wymaganego ustawą okresu przechowywania dokumentacji medycznej przez okres 20 lat. Konieczne jest zatem odnawianie archiwizowanych danych tak, aby spełnić wymogi czasowe ustawy. Zaleca się stosowanie taśm w standardzie LTO-6, które posiadają większą pojemność oraz prędkość transferu danych w stosunku do poprzedniego standardu.
11. System archiwizujący dokumentację medyczną powinien sygnalizować okres przechowywania dokumentacji w celu zakwalifikowania jej do usunięcia.
12. Po upływie wymaganego ustawą [10] czasu przechowywania elektroniczna dokumentacja medyczna powinna zostać zniszczona w sposób uniemożliwiający identyfikację pacjenta, którego dotyczyła. Zasady niszczenia dokumentacji opisane zostały punkcie 3.2.7.

[10] Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. 2016 nr 0 poz. 186),

10. Zarządzanie incydentami związanymi z bezpieczeństwem informacji

Odpowiedzialność: Placówka medyczna, firma zapewniająca usługę SaaS, każdy w swoim zakresie:

- **incydenty powstałe na terenie serwerowni lub związane z urządzeniami serwerowymi, sieciowymi, bezpieczeństwem systemu EDM, danych** – firma zapewniająca usługę SaaS;
- **incydenty powstałe na terenie pomieszczeń placówki medycznej lub związane ze sprzętem komputerowym, wykorzystywanym przez użytkowników** – Placówka medyczna.

Podmiot przechowujący dokumentację medyczną powinien posiadać procedury postępowania na wypadek zdarzeń związanych z naruszeniem bezpieczeństwa. Ma to na celu zwiększenie bezpieczeństwa danych, przechowywanych w systemie.

Zaleca się aby wszyscy pracownicy byli poinformowani o istnieniu procedury dotyczącej zarzadzania incydentami związanymi z bezpieczeństwem informacji i przeszkoleni w zakresie zgłaszania zdarzeń mogących świadczyć o naruszeniu bezpieczeństwa danych, a także potencjalnych słabości systemu informatycznego.

Procedura powinna zawierać następujące zagadnienia:

1. Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji
    - Właściciel systemu we współpracy z Kierownictwem organizacji odpowiada za zapewnienie odpowiednich zasobów dla zgłaszania i obsługi zdarzeń.
    - Każdy Użytkownik/pracownik ma obowiązek niezwłocznego zgłaszania wszystkich zdarzeń mających związek z bezpieczeństwem informacji.
    - Informację o zdarzeniu związanym z bezpieczeństwem informacji należy przekazać osobie odpowiedzialnej za gromadzenie i obsługę zgłoszeń lub wyznaczonej komórce organizacyjnej (np. serwis). Należy ustalić formę komunikacji (mail, telefon, faks, za pośrednictwem systemu zgłoszeniowego).
    - Niedopuszczalne jest, aby zdarzenie mogące mieć wpływ na bezpieczeństwo systemu, danych nie było formalnie zgłoszone, nawet jeśli problem został rozwiązany we własnym zakresie.
    - Osoba odbierająca zgłoszenie dokonuje jego rejestracji oraz przesyła informację zwrotną do osoby zgłaszającej, a następnie dokonuje kategoryzacji zgłoszenia, zostaje przypisana osoba odpowiedzialna.
2. Zarządzanie incydentami związanymi z bezpieczeństwem informacji

- Osoba odpowiedzialna rozwiązuje problem, dokonuje adnotacji o sposobie jego rozwiązania oraz przesyła informację do osoby zgłaszającej incydent oraz zamyka zgłoszenie.
- Osoba odpowiedzialna za rozwiązanie problemu dokonuje analizy zgłoszenia, w przypadku braku uprawnień lub kompetencji do podjęcia stosownych działań eskaluje problem na wyższy poziom, zależnie od przyjętej struktury obsługi zgłoszenia.
- W przypadku gdy konieczne jest przekierowanie zgłoszenia do podmiotu zewnętrznego (np.: wykonawcy systemu) należy dokonać dodatkowej kategoryzacji, zgodnie z umowa obowiązującą z podmiotem zewnętrznym. Gdy zdarzenie ma istotny wpływ na funkcjonowanie systemu lub nie jest możliwe wprowadzenie działań naprawczych w krótkim czasie, należy poinformować Właściciela systemu.

3. Postępowanie dyscyplinarne

- W przypadku pracowników, którzy naruszyli obowiązujące zasady bezpieczeństwa zaleca się stosowanie formalnego postępowania dyscyplinarnego. Takie postepowanie powinno być prowadzone wyłącznie po zgromadzeniu dowodów, po upewnieniu się, że nastąpiło naruszenie oraz stopniowane w zależności od rodzaju, wagi naruszenia, okoliczności, czy pracownik został wcześniej przeszkolony, itd.
- Sankcje w stosunku do osób, które naruszyły procedury bezpieczeństwa powinny być jasno określone. Postępowanie dyscyplinarne ma stanowić również swego rodzaju środek odstraszający dla pracowników, którzy byliby skłonni do lekceważenia zasad bezpieczeństwa.
- Postepowanie prowadzi się zgodnie z obowiązującymi przepisami, w tym m.in.: Kodeksu Pracy oraz regulaminu organizacji oraz przepisami szczególnymi dotyczącymi pracowników, w zależności od danego podmiotu. Dla przykładu, osobie, która naruszyła zasady bezpieczeństwa może grozić pouczenie lub nagana, w myśl przepisów Kodeksu Pracy.
- Zaleca się, aby w przypadku poważnego naruszenia zasad bezpieczeństwa przez pracownika możliwe było jego natychmiastowe zwolnienie z obowiązków oraz odebranie praw dostępu.
- Ponadto, w przypadku gdy naruszenie zasad bezpieczeństwa prowadzi do szkody po stronie pracodawcy, może on dochodzić odszkodowań zgodnie z przepisami prawa pracy. Jeśli natomiast naruszenie bezpieczeństwa jest jednocześnie czynem zabronionym, w myśl przepisów karnych, pracodawca jest zobowiązany zgłosić zawiadomienia o popełnieniu przestępstwa do właściwych organów.

- W stosunku do osób, które naruszyły zasady bezpiecznego przechowywania danych osobowych zastosowanie mają również przepisy rozdziału 8 ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997r. odpowiedzialności karnej (Dz.U. 2016 nr 0 poz. 922),,
- W przypadku gdy działania podejmowane po wystąpieniu incydentu bezpieczeństwa wymagają użycia kroków prawnych, należy gromadzić, przechowywać oraz przedstawić materiał dowodowy zgodnie z obowiązującym prawem,
- Zaleca się, aby w organizacji istniały mechanizmy służące do analizy incydentów związanych z bezpieczeństwem informacji (np.: rodzajów, rozmiarów i kosztów incydentów), co umożliwi wyciągnie odpowiednich wniosków.

11. Zarządzanie ciągłością działania

Odpowiedzialność: Placówka medyczna, Firma zapewniająca usługi SaaS

Zarządzanie ciągłością działania ma na celu ochronę prowadzonej działalności oraz krytycznych procesów, a tym samym przetwarzanych danych przed awariami systemów informatycznych lub katastrofami oraz zminimalizowanie skutków wystąpienia przerw w pracy tych systemów, braku dostępności danych. W związku z tym niezbędne jest wdrożenie w organizacji procesu zarzadzania ciągłością działania, który w szczególności obejmuje:

- Wskazanie krytycznych procesów dla działalności biznesowej oraz przeprowadzenie analizy ryzyka dla systemu EDM i wskazanie na tej podstawie wszystkich aktywów biorących udział w tych procesach,
- Wdrożenie niezbędnych zabezpieczeń,
- Stworzenie oraz regularne przeglądanie, doskonalenie planów ciągłości działania. Na podstawie powyższych analiz, Administrator systemu powinien opracować i wdrożyć plany ciągłości działania, które będą zawierały instrukcje i procedury niezbędne na wypadek konieczności utrzymania lub przywrócenia systemu w sytuacji awaryjnej. Plany powinny w szczególności zawierać:
    - Zasady bezpiecznej eksploatacji systemu;
    - Zasady tworzenia kopii zapasowych;
    - Zasady postępowania w sytuacjach awaryjnych, nietypowych.

Procedury zapewniające ciągłość działania systemu powinny być zaakceptowane przez właściciela systemu, a następnie odpowiednie osoby powinny zostać z nimi zapoznane,

Testowanie oraz aktualizowanie planów ciągłości działania. Zalecane jest przeprowadzanie okresowych testów nie rzadziej niż raz na rok, w uzasadnionych przypadkach, np.: wprowadzanie istotnych zmian w systemie, każdorazowo po wprowadzeniu takiej zmiany.

Rezultat testów powinien być odzwierciedlony w raporcie, który następnie przestawiany jest Właścicielowi systemu. W przypadku stwierdzenia rozbieżności pomiędzy stanem zakładanym, a rzeczywistym Właściciel systemu podejmuje działania mające na celu aktualizację planów.

11.1. Tworzenie i odtwarzanie kopii zapasowych

Odpowiedzialność: Firma zapewniająca usługi SaaS

1. Wszystkie newralgiczne dane umożliwiające odtworzenie systemu po awarii powinny być poddawane procesowi tworzenia kopii bezpieczeństwa. Dotyczy to:
    - Danych w bazach danych;
    - Systemu operacyjnego;
    - Aplikacji;
    - Oprogramowania narzędziowego zainstalowanego na serwerze.

    Dodatkowo zaleca się wykonywać kopie zapasowe plików konfiguracyjnych, logów systemowych, dzienników zdarzeń.
2. Proces tworzenia kopii zapasowych musi być skonfigurowany w taki sposób, aby w razie awarii możliwe było pełne odtworzenie systemu.
3. Dla każdego systemu podlegającego procedurze tworzenia kopii zapasowych powinna istnieć instrukcja odtwarzania systemu. Na jej podstawie powinno być możliwe odtworzenie pełnej konfiguracji systemu, łącznie z systemem operacyjnym.
4. Proces tworzenia kopii zapasowych należy przeprowadzić zgodnie z instrukcją znajdującą się w dokumentacji technicznej systemu lub aplikacji.
5. Ze względu bezpieczeństwa zaleca się tworzenie dwóch kopii zapasowych i przechowywanie ich w różnych miejscach, jedna z kopii powinna być przechowywana poza siedzibą organizacji, w której uruchomiona jest podstawowa instalacja systemu EDM oraz przechowywana i przetwarzana jest dokumentacja medyczna.
6. Kopie zapasowe należy tworzyć przynajmniej w następującym cyklu:
    a. Baza danych – pełny backup raz w tygodniu (np. w weekend), raz na dzień, w ciągu tygodnia backup przyrostowy lub różnicowy;
    b. System operacyjny – pełny backup raz w tygodniu (np. w weekend);
    c. Aplikacja – pełny backup raz w tygodniu (np. w weekend);

d. Oprogramowanie narzędziowe – pełny backup raz w tygodniu (np. w weekend).

7. Kopie baz danych powinny być zabezpieczone przed nieuprawnionym dostępem (np.: kontrola dostępu i szyfrowanie danych).
8. Okres przechowywania kopi zapasowych wynosi 3 miesiące. Po ustaniu użyteczności kopii zapasowych należy je niezwłocznie usunąć. Po upływie okresu przechowywania najstarszy nośnik może być wykorzystany ponownie. Należy jednak zadbać o to, aby dane wcześniej na nim zapisane zostały skutecznie usunięte. Wykorzystując ponownie ten sam nośnik bezwzględnie weryfikować należy poprawność zapisu i możliwość odczytania jego zawartości. Umożliwi to uniknięcie sytuacji, w której mimo przeprowadzenia procesu backupu nie mamy dostępu do zapisanych danych.
9. Kopie zapasowe powinny być przechowywane w miejscu bezpiecznym, zapewniającym ochronę przed dostępem osób nieuprawnionych, modyfikacją, uszkodzeniem, zniszczeniem oraz wpływem środowiska.
10. Co najmniej jedna z dwóch kopii zapasowych powinna być trzymana w innej lokalizacji niż podstawowa instalacja systemu..
11. Kopie zapasowe powinny być regularnie testowane. Zaleca się wykonywanie okresowych testów odtwarzania systemu i aplikacji z backupu. Zaleca się testowanie wszystkich kopii bezpieczeństwa przynajmniej raz na rok.
12. Proces odtwarzania systemu z backupu należy przeprowadzić zgodnie z instrukcją odtwarzania systemu. Instrukcja taka powinna być elementem dokumentacji dostarczonej z systemem.
13. Po ustaniu użyteczności kopii zapasowych należy je niezwłocznie usunąć, w sposób trwały i bezpieczny.

11.2. Dostępność i niezawodność (SLA)

Odpowiedzialność: Firma zapewniająca usługę SaaS

Z punktu widzenia zachowania ciągłości działania podmiotu przetwarzającego dane medyczne niezbędne jest zapewnienie odpowiedniej asysty technicznej dla sprzętu i oprogramowania.

W tym celu należy zawrzeć pisemną umowę gwarantującą odpowiedni poziom usług świadczonych przez podmioty zewnętrzne realizujące usługi asysty na sprzęt i oprogramowanie.

1. Właściciel systemu jest zobowiązany do określenia warunków SLA.
2. Wymagania SLA powinny określać m.in.:
    a. Czas dostępności usługi;
    b. Dopuszczalny czas przerwy w świadczeniu usługi;

   c. Czas reakcji na zgłoszenie, czas podjęcia naprawy, czas przywrócenia wymaganego poziomu usług.

3. Umowy SLA powinny być podpisywane z podmiotami posiadającymi odpowiednie uprawnienia i kwalifikacje.
4. Należy monitorować i egzekwować wymagania dotyczące poziomu usług, zgodnie z umową.
5. Umowy SLA powinny obejmować wszystkie elementy systemu, których awaria może spowodować poważne konsekwencje w funkcjonowaniu systemu. Dotyczy to w szczególności:
   a. Infrastruktury sieciowej;
   b. Infrastruktury sprzętowej (w tym UPS);
   c. Systemów i aplikacji;
   d. Usług telekomunikacyjnych;
   e. Usług przeglądów technicznych;
   f. Klimatyzacji, systemu gaśniczego, systemu zasilania.
6. Należy zidentyfikować i opracować pełną listę umów, definiujących warunki SLA. Lista taka powinna być częścią Polityki Bezpieczeństwa.
7. Umowa z firmą świadczącą usługi asysty powinna w razie nie wywiązania się z ze zobowiązań gwarantować odpowiednie rekompensaty finansowe. W przypadku niedotrzymania warunków SLA należy uzgodnić działanie naprawcze.
8. Wszystkie umowy SLA powinny być regularnie przeglądane i aktualizowane.

11.3. Postępowanie na wypadek awarii/katastrofy i utraty danych

Odpowiedzialność: Placówka medyczna, Firma zapewniająca usługi SaaS

1. Podmiot przetwarzający dane medyczne powinien opracować plan na wypadek wystąpienia poważnych awarii systemu, uszkodzeń, utraty danych, w wyniku np. pożaru, powodzi, itd.
2. W przypadku wystąpienia zdarzenia, które uniemożliwia zachowanie ciągłości działania systemu EDM należy uruchomić procedurę odtwarzania systemów po katastrofie. Przywracane są wówczas kluczowe funkcje systemu, w możliwie najkrótszym czasie.
3. Procedury odtwarzania systemów po katastrofie podlegają regularnym przeglądom.
4. Należy przygotować odpowiednie działania na wypadek konieczności odtwarzania systemu:

a. Regularne, zgodne z procedura tworzenie kopii zapasowych systemów, aplikacji, konfiguracji;

b. Właściwe przechowywanie kopii zapasowych;

c. Stworzenie oddalonego geograficznie ośrodka przetwarzania danych;

d. Zapewnienie odpowiedniego poziomu usług SLA w stosunku do newralgicznych punktów systemu;

e. Stworzenie szczegółowych procedur odtwarzania systemów, które powinny zawierać szczegółowe kroki związane z odtworzeniem systemu, wskazanie lokalizacji wszystkich zasobów niezbędnych do odtworzenia systemu, wskazanie osób odpowiedzialnych za jego wykonanie, dane kontaktowe do osób uczestniczącym w działaniach kryzysowych (m.in. Kierownictwo, służby publiczne, dostawcy usług SLA itd.);

f. Przygotowanie zapasowych pomieszczeń przeznaczonych do odtwarzania systemu,

5. W razie wystąpienia sytuacji kryzysowej powoływany jest zespół kryzysowy, który wraz z Właścicielem systemu i Koordynatorem Działań Kryzysowych ocenia sytuację, wymagane działania oraz ich priorytety.

6. Koordynator Działań Kryzysowych wraz z Właścicielem systemu oraz Sztabem kryzysowym podejmuje decyzję o uruchomieniu procedury odtwarzania systemu i powiadamia odpowiednie zespoły realizujące. Jest również odpowiedzialny za przeprowadzenie działań związanych z odtworzeniem systemu, kieruje pracą wszystkich zespołów.

7. Działania, jakie należy podjąć w pierwszej kolejności to:

   a. Zapewnienie właściwych warunków zasilania;

   b. Zapewnienie właściwych warunków środowiskowych, w szczególności klimatyzacja, wentylacja, itd.;

   c. Zapewnienie działania infrastruktury sieciowej.

   Zadania, o których mowa powyżej, powinny być określone w szczegółowych procedurach.

8. Dane medyczne przechowywane w systemie muszą być zabezpieczone przed utratą poufności, przed nieuprawnionym dostępem nawet w przypadku katastrofy lub klęski żywiołowej.

9. W przypadku wystąpienia konieczności przeprowadzenia ewakuacji, osoby mające kontakt z systemem powinny w miarę możliwości zabezpieczyć system przed nieuprawnionym dostępem, np. zabrać ze sobą kartę z certyfikatem. Powyższego zalecenia nie stosuje się w przypadku gdy czynności te mogłyby stanowić zagrożenie życia lub zdrowia użytkowników systemu.

12. Działania dodatkowe

Odpowiedzialność: Placówka medyczna, firma zapewniająca usługę SaaS, każdy w swoim zakresie zgodnie z opisem poniżej.

Zadania realizowane we własnym zakresie lub zlecane na zewnątrz:

1) **Przegląd, wybór metod i środków ochrony dokumentacji, których skuteczność w czasie ich zastosowania jest powszechnie uznawana oraz przygotowanie i realizacja planów przechowywania dokumentacji w długim czasie, w tym jej przenoszenia na nowe informatyczne nośniki danych i do nowych formatów danych, jeżeli tego wymaga zapewnienie ciągłości dostępu do dokumentacji**

Odpowiedzialność: Firma zapewniająca usługę SaaS

Wprowadzenie elektronicznego sposobu gromadzenia i przetwarzania dokumentacji medycznej wiązało się będzie z wprowadzeniem mechanizmów utrzymania tej dokumentacji. Utrzymanie to nie tylko ochrona danych przed utratą, nieuprawnionym odczytem i zmianą, ale również, podobnie jak dotychczas w przypadku prowadzenia dokumentacji w postaci papierowej, dbałość o przechowywanie i możliwość jej odczytu. W początkowym okresie problem odczytu nie będzie aż tak istotny, jednak tempo rozwoju technologii spowoduje potrzebę konwersji dokumentacji medycznej z obecnych, uznanych dzisiaj jako standardy formatów danych do nowych. W przypadku dokonania np. zmian w infrastrukturze systemowo-sprzętowej istotne jest, aby dane z archiwum przenieść na nośniki fizyczne, z których będzie można pozyskać dane zapisane wcześniej. Istotna jest tu zarówno zgodność sprzętowa rozwiązań, jak również zabezpieczenie przed skutkami utraty trwałości nośnika wynikającymi z upływającego czasu czy też zużycia. Dlatego też wskazane jest regularne dokonywanie przeglądów wymagań i wytycznych w zakresie elektronicznej dokumentacji medycznej i wprowadzanie wynikających z nich zmian.

2) **Systematyczne dokonywanie analizy zagrożeń**

Odpowiedzialność: Firma zapewniająca usługę SaaS

Jest to proces nieoderwalnie związany z utrzymaniem i rozwojem systemu jak również procedur związanych z przetwarzaniem dokumentacji medycznej. Zadanie to powinno być realizowane w stałych, przyjętych cyklach. Analiza zagrożeń powinna być dodatkowo prowadzona na etapie przygotowania do wdrożenia zmian systemu teleinformatycznego lub procedur wewnętrznych organizacji. Analiza ma zidentyfikować miejsca systemu czy procedur potencjalnie narażone na działania niepożądane. Prowadzona analiza ma pomóc w przygotowaniu mechanizmów eliminacji zagrożeń.

3) **Opracowanie i stosowanie procedur zabezpieczania dokumentacji i systemów ich przetwarzania, w tym procedur dostępu oraz przechowywania**

Odpowiedzialność: Firma zapewniająca usługę SaaS

Podobnie jak dla dokumentacji w postaci papierowej należy dokładać wszelkiej staranności w obszarze zabezpieczania i przetwarzania dokumentacji elektronicznej. Podstawowym elementem jest opracowanie i wdrożenie przejrzystych, czytelnych, zgodnych z normami i wymaganiami prawnymi, spójnych, zrozumiałych dla personelu procedur. Dodatkowo, wymagane jest systematyczne (np. przy okazji prowadzonych w cyklu rocznym audytów) dokonywanie przeglądu procedur i sposobu ich egzekwowania. Należy dołożyć wszelkich starań, aby procedury były przestrzegane.

4) **Stosowanie środków bezpieczeństwa adekwatnych do zagrożeń**

Odpowiedzialność: Firma zapewniająca usługę SaaS

Efektem wcześniej opisanej, regularnie prowadzonej analizy ryzyka powinna być lista zidentyfikowanych ew. podatności systemów teleinformatycznych lub procedur mogących prowadzić do wystąpienia zagrożeń. Żadne z nich nie powinno być zlekceważone i dla każdego powinny zostać przewidziane środki zaradcze, które minimalizować będą możliwość jego wystąpienia. Adekwatny dobór środków zaradczych polega na takim dopasowaniu mechanizmu zapobiegawczego, który w optymalny - finansowy, proceduralny i techniczny - sposób przeciwdziała zidentyfikowanemu zagrożeniu.

5) **Bieżące kontrolowanie funkcjonowania wszystkich organizacyjnych i technicznoinformatycznych sposobów zabezpieczenia, a także okresowe dokonywanie oceny skuteczności tych sposobów**

Odpowiedzialność: Placówka medyczna, Firma zapewniająca usługę SaaS

Utrzymując system teleinformatyczny we własnym zakresie podmiot zobowiązany jest do regularnego monitorowania zachowań systemu i jego użytkowników oraz przestrzegania wprowadzonych procedur. Zadanie to jest typowe dla zadań realizowanych przez zespoły utrzymaniowe i powszechnie znane. Realizacja tych zadań poddawana jest najczęściej ocenie przy okazji wykonywania audytów. Prowadzone kontrole powinny oceniać sposób funkcjonowania zabezpieczeń w organizacji poprzez m.in. porównanie postawionych celów i sposobu ich osiągniecia. Szczególnie istotne jest systematyczne prowadzenie kontroli przy korzystaniu z usług kolokacji, chmury lub innej, w której część zadań powierzanych jest na zewnątrz.

6) **Zapewnienie monitorowania i aktualizacji zastosowanych środków bezpieczeństwa, wprowadzenie spójnych i egzekwowalnych zasad.**

Odpowiedzialność: Firma zapewniająca usługę SaaS

Niezależnie od przyjętego modelu korzystania z usług związanych z przetwarzaniem elektronicznej dokumentacji medycznej, realizowanego we własnym zakresie czy korzystania z usług pochodzących od zewnętrznych dostawców, bezwzględnie należy zadbać o najwyższy poziom ich bezpieczeństwa. Dla usług realizowanych w ramach jednostki, należy opracować i wdrożyć (we własnym zakresie lub wykorzystując doświadczony podmiot zewnętrzy) odpowiednie procedury określające obowiązki nakładane na administratorów i użytkowników systemu, z jednoczesnymi regulaminowo określonymi

sankcjami. Należy również opracować i wprowadzić reguły badania i weryfikacji przestrzegania obowiązujących procedur.

W przypadku wyniesienia części usług poza organizację należy zadbać o odpowiednie zapisy umowne, z jednej strony narzucające na podmiot realizujący umowę dokładnie sprecyzowane, rozliczalne warunki i z drugiej, dające możliwość pełnej kontroli i monitoringu dla zlecającego. Ujmowanie takich regulacji w umowach powinno być normą i dotyczyć wszystkich usług realizowanych na potrzeby organizacji.

7) Szkolenia dla personelu z zakresu bezpiecznego przetwarzania dokumentacji

Odpowiedzialność: Placówka medyczna**.**

Szkolenia personelu są niezbędnym elementem skutecznego wdrożenia procedur, wytycznych i regulacji przyjętych w danej jednostce. Należy zadbać o to, aby był przygotowany i realizowany coroczny plan szkoleń obejmujący wszystkie funkcjonujące w jednostce poziomy zatrudnienia. Istotne jest także, aby wiedza przekazywana na szkoleniach była weryfikowana np. poprzez wew. egzaminy. W zależności od wielkości jednostki, liczby zatrudnianych i fluktuacji kadr, szkolenia mogą być realizowane w kilku modelach. Szkolenia mogą być realizowane w klasyczny stacjonarny sposób, jednak coraz częściej wykorzystuje się szkolenia elektroniczne (*ang. e-learning*).

8) Przeprowadzanie audytów wewnętrznych i zewnętrznych

Odpowiedzialność: Placówka medyczna, Firma zapewniająca usługę SaaS

Każda jednostka jest zobowiązana do prowadzenia i poddawania się regularnym audytom. Zakres audytów został szczegółowo omówiony we wcześniejszych rozdziałach, jednak ze względu na ważność tego elementu, każda jednostka powinna przygotowywać coroczny plan audytu i rezerwować w swoich budżetach odpowiednie środki na ten cel. Regularność audytów jest szczególnie istotna w przypadku jednostek posiadających certyfikaty jakości ale również dla tych, które mimo braku certyfikatów dbają o wysoki poziom realizowanych usług.

9) Opracowywanie własnych zaleceń mających wpływ na poprawienie procesów przetwarzania dokumentacji w organizacji.

Odpowiedzialność: Placówka medyczna, Firma zapewniająca usługę SaaS

W opracowaniu wymieniono szereg ustawowych, pochodzących z krajowych i światowych norm obowiązków związanych z bezpiecznym przetwarzaniem danych. Zakres tych regulacji jest obowiązujący dla wszystkich jednostek, jednak zalecane jest również korzystanie z dobrych praktyk innych jednostek czy specjalistycznych firm i wprowadzanie ich do własnej organizacji. Sprawdzone mechanizmy i procesy zarządzania, niekoniecznie wynikające wprost z regulacji prawnych, adoptowane na własny użytek, są często kluczem do sukcesu sprawnego przetwarzania danych medycznych i związanej z nimi dokumentacji.

10) Utrzymanie i konserwacja infrastruktury teleinformatycznej

Odpowiedzialność: Firma zapewniająca usługę SaaS

Realizując zadanie utrzymania systemu teleinformatycznego wspomagającego obsługę elektronicznej dokumentacji medycznej lub w przypadku mniejszych jednostek, które korzystają z usług zewnętrznych w zakresie EDM, należy w odpowiedni sposób zadbać o jakość posiadanej infrastruktury teleinformatycznej i zabezpieczyć się na wypadek uszkodzenia. Dobrą praktyką w tym zakresie jest posiadanie umów serwisowych z podmiotami zewnętrznymi, które gwarantują konserwację, dostępność i wymianę sprzętu oraz oprogramowania w krótkim, nie wpływającym na poziom obsługi pacjentów czasie. Należy również wykazywać się daleko idąca dbałością o aktualizację i wymianę sprzętu po okresie jego używalności. Ma to bezpośrednie przełożenie na bezpieczeństwo i niezawodność realizowanych usług.

Zadania realizowane we własnym zakresie:

Odpowiedzialność: Placówka medyczna

1 **Umowy gwarantujące wysoki poziom usług.**

Decydując się na korzystanie z usług pochodzących od zewnętrznych dostawców należy zadbać o należyte zabezpieczenie własnych interesów i wysoki poziom oferowanych usług. Warto umieszczać w umowach jasno określone wymagania w zakresie dostępności, niezawodności i jakości usług, terminów usuwania zidentyfikowanych błędów i problemów oraz konsekwencje finansowe ich niedotrzymywania. Należy także oczekiwać od dostawców określenia i zapewnienia kanałów bezpośredniego wsparcia np. helpdesk, szkoleń i innych elementów zapewniających kompletność oferowanych usług, w tym zapewnienie zgodności oferowanych usług ze zmieniającym się prawem.

2) Planowanie budżetu.

Zakup sprzętu, budowa systemu, wynajęcie powierzchni czy abonament usługi wiąże się z poniesieniem określonych kosztów. Należy jednak pamiętać, że podjęcie decyzji o realizacji którejś z wymienionych inwestycji jak również spełnienie wymogów wynikających z prawa wymaga długoterminowego planowania budżetu. Istotne jest coroczne zapewnienie odpowiednich środków, bez których zapewnienie wysokiego poziomu świadczonych usług, czy nawet korzystanie z usług zewnętrznych będzie niemożliwe. Należy pamiętać o egzekwowaniu od dostawców zewnętrznych systemów, elementów infrastruktury, licencji dokładnego określenia przyszłych kosztów eksploatacyjnych. Często bowiem zdarza się, że w dostarczanych ofertach świadomie pomijane są pewne elementy, które uzależniają podmiot od określonego, jednego dostawcy.

3) Dbałość o bezpieczeństwo i egzekwowanie regulacji wewnętrznych.

Bezpieczeństwo systemu i organizacji jest uzależnione od wielu czynników. Zostały one szeroko opisane w niniejszym opracowaniu. Warto zwrócić uwagę na to, aby w budowę i wdrażanie dobrych praktyk w zakresie bezpieczeństwa, budowanych na bazie niniejszego opracowania, angażowane było kierownictwo jednostek. Takie podejście przyczyni się do podniesienia świadomości osób decyzyjnych oraz innych poziomów kadry w organizacji. Dzięki temu możliwe będzie wdrażanie rozwiązań

ułatwiających stosowanie się do wytycznych dotyczących zachowania bezpieczeństwa. Kadra zarządzająca musi zdawać sobie sprawę z odpowiedzialności, jaka na niej spoczywa oraz bezwzględnie uznawać decyzyjność takich ról jak: Administrator Bezpieczeństwa Informacji w zakresie stosowania polityki bezpieczeństwa i instrukcji zarządzania systemem przetwarzania danych. Na każdym poziomie zatrudnienia muszą być przestrzegane wprowadzone regulacje, a w stosunku do osób naruszających bezpieczeństwo muszą być wyciągane konsekwencje w nich przewidziane.