POLITYKA BEZPIECZEŃSTWA DLA PARTNERÓW

Metryka dokumentu			
Umowa nr	IXA/12/IS/23		
Zamawiający	Województwo Małopolskie		
Partner Projektu	Comarch S.A. (Lider konsorcjum)		
Kod i nazwa produktu	PS_MSIM2_E4-1-15-S Polityka bezpieczeństwa dla Partnerów		
Kierownik Partnera Projektu	Jarosław Brzeziński	Status dokumentu	Zatwierdzony
Wersja	2.00	Data wersji	14.11.2024
Autor	Patryk Kozłowski	Ilość stron	18

Historia zmian dokumentu			
Wersja	**Data**	**Treść / Zmiana**	**Autor**
0.10	01.06.2023	Produkt przekazany do weryfikacji	Wykonawca
0.11	19.06.2023	Produkt przekazany do ponownej weryfikacji po wdrożeniu uwag Zamawiającego.	Wykonawca
0.12	14.07.2023	Produkt przekazany do ponownej weryfikacji po wdrożeniu uwag Zamawiającego.	Wykonawca
0.13	03.08.2023	Produkt przekazany do ponownej weryfikacji po wdrożeniu uwag Zamawiającego.	Wykonawca
0.20	18.09.2023	Produkt przekazany do ponownej weryfikacji po wdrożeniu uwag Zamawiającego.	Wykonawca
0.30	03.10.2023	Produkt przekazany do ponownej weryfikacji po wdrożeniu uwag Zamawiającego.	Wykonawca
0.40	05.10.2023	Produkt przekazany do ponownej weryfikacji po wdrożeniu uwag Zamawiającego.	Wykonawca
0.50	16.10.2023	Produkt przekazany do ponownej weryfikacji po wdrożeniu uwag i sugestii Zamawiającego.	Wykonawca
1.00	17.10.2023	Produkt zatwierdzony	Zamawiający
1.10	05.07.2024	Poszerzenie zapisów o obszar ustawy o Prawach Pacjenta	Wykonawca
1.11	14.11.2024	Aktualizacja dokumentacji w związku z realizacją Zlecenia nr. 1	Wykonawca
2.00	14.11.2024	Produkt zatwierdzony	Zamawiający

Spis treści

1 Cel dokumentu

1. Celem niniejszego dokumentu, zwanego dalej *Polityką* jest zapewnienie bezpieczeństwa przetwarzanych danych osobowych oraz systemów Platformy MSIM, określenie minimalnych zasad bezpieczeństwa i ochrony danych osobowych podczas korzystania z systemów Platformy, jak również sposobów weryfikacji, w jaki sposób te zasady są realizowane. Dokument powstał na bazie Polityki Bezpieczeństwa i Ochrony Danych Osobowych dla Platformy MSIM i zawiera wybrane aspekty bezpieczeństwa informacji, jakich wymaga się od Partnerów Projektu w celu zapewnienia poufności, dostępności i integralności przetwarzanych w ramach Platformy danych i informacji.

2 Zakres stosowania

1. Niniejsza Polityka obowiązuje wszystkich pracowników i współpracowników Partnerów Projektu MSIM (np. m.in. współpracujących w ramach umów cywilnoprawnych, wolontariatów, praktyk czy staży zawodowych), uzyskujących dostęp, przetwarzających, przechowujących, przesyłających, modyfikujących, dostarczających czy odczytujących informacje przetwarzane w ramach Platformy MSIM. Ilekroć w niniejszej polityce mowa jest o Pracowniku Partnera należy przez to rozumieć też współpracownika. Wymagania opisane w niniejszym dokumencie stosuje się do wszystkich modułów, wszystkich Portali wytworzonych w ramach Platformy. Postanowienia niniejszej Polityki stosowane są we wszystkich umowach zawartych między Urzędem Marszałkowskim Województwa Małopolskiego a Partnerami Projektu – Podmiotami Leczniczymi w zakresie ochrony informacji przetwarzanych na Platformie MSIM.

2. Z niniejszej Polityki wyłączone są:
   a) informacje niejawne oraz dedykowane systemy przetwarzania informacji niejawnych, dla których stosowane są odrębne przepisy (tj. np. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych lub aktualne w tym zakresie).
   b) Portal Pacjenta – który z zakresie zapewnienia bezpieczeństwa rozwiązania objęty jest regulacjami opisanymi w Polityce Bezpieczeństwa i Ochrony Danych Osobowych dla Platformy MSIM, a w obszarze bezpiecznego użytkowania, adekwatne zasady dla Pacjentów definiuje Regulamin Portalu Pacjenta.

3 Postanowienia ogólne

1. Niniejsza Polityka określa zakres obowiązków i odpowiedzialności Partnerów w zakresie bezpieczeństwa informacji przetwarzanych w ramach Platformy. Obejmuje swym zakresem wszystkich Partnerów Projektu, mających dostęp do systemów informacyjnych wytworzonych w ramach Platformy MSIM. Polityka jest syntezą informacji zawartych w Polityce Bezpieczeństwa Informacji i Ochrony Danych Osobowych opracowanej w ramach tworzenia Platformy MSIM i przedstawia wymagania i dobre praktyki jakie należy stosować korzystając z Platformy.
2. Partner Projektu:
   a) odpowiada za zapewnienie łączności pomiędzy Lokalnym Repozytorium Danych Medycznych a Platformą;
   b) odpowiada za wdrożenie i stosowanie odpowiednich mechanizmów bezpieczeństwa dla własnego repozytorium;
   c) nadzoruje pracę własnego personelu w obszarze stosowania przez nich postanowień polityk bezpieczeństwa;

d) jest Administratorem Danych Osobowych (w ustalonym zakresie).

3. Z niniejszej Polityki wyłączone są systemy dziedzinowe Partnerów Projektu oraz Infrastruktura je utrzymująca. Polityka może wskazywać kierunki poprawy własnego środowiska IT, lecz w zakresie własnym Partnerzy Projektu powinni opracować wewnętrzne zasady bezpieczeństwa ich infrastruktury i je stosować. Mogą natomiast posiłkować się wskazówkami zawartymi w niniejszym dokumencie do wyznaczania kierunków poprawy.
4. Zalecanym jest, by Partnerzy Projektu stosowali się do wymagań niniejszej Polityki w ramach korzystania z Platformy MSIM. Partnerom Projektu rekomenduje się następujące działania, które należy przeprowadzić w ciągu pierwszych 3 miesięcy korzystania z Platformy:
   a) Zapoznanie pracowników i osób trzecich, realizujących w imieniu Partnera zadania w ramach działania Platformy, w zakresie zachowania zasad bezpieczeństwa informacji,
   b) każda osoba, która w imieniu Partnera Projektu bezpośrednio uczestniczy w realizacji przedmiotu Umowy z Właścicielem Platformy MSIM zobowiązana jest do zapoznania się z niniejszą Polityką i podpisania przed przystąpieniem do realizacji zadań, imiennego oświadczenia, którego wzór stanowi załącznik nr. 1 do niniejszej Polityki. Podpisane oświadczenia przechowywane są przez Partnera Projektu.
5. Podstawą prawną przetwarzania danych osobowych przez Partnerów Projektu w odniesieniu do danych:
   a. Pacjentów - są art. 6 ust. 1 lit. c i art. 9 ust. 2 lit. h. RODO, które umożliwiają przetwarzanie danych, gdy jest to niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej Obowiązek prawny przetwarzania danych osobowych pacjentów wynika z ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (t.j. Dz. U. z 2024 r. poz. 581), w szczególności art. 24 powołanej ustawy.;
   b. lekarzy, pracowników i osób trzecich, realizujących w imieniu Partnera zadania w ramach działania Platformy - art. 6 ust. 1 lit. c. RODO, który umożliwia przetwarzanie danych niezbędnych do wypełnienia obowiązku prawnego ciążącego na administratorze.

4 Dostęp do Środowiska teleinformatycznego Platformy

1) Partner Projektu zobowiązany jest wykorzystywać przyznany dostęp wyłącznie w celach i w zakresie uzasadnionym realizacją zadań wynikających z obowiązujących przepisów prawa oraz właściwego rodzaju Umowy (np. Partnerskiej, Powierzenia czy Eksploatacji).
2) Partner Projektu zobowiązany jest zapewnić właściwą ochronę udostępnionych mu przez Właściciela Platformy systemów lub zasobów informacyjnych, polegającą w szczególności na zapewnieniu zespołu środków organizacyjnych, technicznych i prawnych stosowanych w celu zapewnienia bezpieczeństwa informacji.
3) Dostęp do serwerów zarządzających działaniem Platformy MSIM realizowany jest wyłącznie z użyciem stacji przesiadkowych udostępnianych przez Podmiot Utrzymujący Platformę na zlecenie Podmiotu Zarządzającego. Sesje takie są izolowane i monitorowane w czasie rzeczywistym.
4) W związku z dostępem do środowiska teleinformatycznego Platformy, Partner Projektu ma obowiązek stosować się do zaleceń oraz rekomendacji Podmiotu Zarządzającego, mających na celu zapewnienie bezpieczeństwa informacji, m.in. poprzez:
   a) Zapoznanie własnego personelu z wymaganiami bezpieczeństwa opisanymi w politykach bezpieczeństwa;
   b) Zapewnienie przestrzegania zasad bezpiecznego korzystania systemów teleinformatycznych Platformy opisanych w politykach bezpieczeństwa
   c) Zapewnienie przestrzegania zasad bezpiecznej pracy.

5) Partner Projektu jednocześnie zapewnia, że dostęp do systemów lub zasobów teleinformatycznych Platformy będą posiadać wyłącznie uprawnieni i przeszkoleni pracownicy/współpracownicy, w zakresie i na czas niezbędny do realizacji przez nich przedmiotu Umowy (Partnerskiej, Powierzenia czy Eksploatacji).
6) Za sprawowanie nadzoru nad korzystaniem przez Pracowników Partnera Projektu z dostępu do systemów lub zasobów teleinformatycznych odpowiada kierownictwo Partnera Projektu. Bez uszczerbku dla postanowień Umowy, Partner Projektu ponosi pełną odpowiedzialność za działania swoich pracowników/współpracowników w systemach lub zasobach teleinformatycznych Platformy oraz za wszelkie szkody powstałe w związku z korzystaniem przez Pracowników Partnera Projektu z dostępu do systemów lub zasobów teleinformatycznych Platformy w sposób sprzeczny z niniejszą Polityką.
7) W sytuacji korzystania z zasobów Platformy przez Partnerów Projektu, Partner Projektu zapewnia przestrzeganie przez Podmioty realizujące zlecenia związane z Platformą oraz osoby realizujące w ich imieniu Umowy zawarte z Partnerem (np. na integrację z Platformą) wszystkich wymagań bezpieczeństwa w ramach Platformy, o których mowa w niniejszej Polityce i ponosi w tym zakresie pełną odpowiedzialność przed Właścicielem Platformy, a pośrednio względem Podmiotu Zarządzającego Platformą.
8) Niedozwolone jest łączenie się w trybie administracyjnym z publicznie dostępnych sieci, obiektów otwartych typu galerie handlowe, kawiarnie czy środki transportu publicznego, gdyż istnieje ryzyko nieświadomego ujawnienia danych (w tym danych wrażliwych).

5 Zarządzanie uprawnieniami

1) Dostęp Pracowników Partnera Projektu do środowiska teleinformatycznego Platformy odbywa się wyłącznie na zasadach określonych w niniejszej Polityce. Uprawnienia przyznaje się Pracownikom Partnera Projektu po podpisaniu Umowy (Partnerskiej, Powierzenia czy Eksploatacji).

2) Uprawnienia przyznawane są Pracownikom Partnera Projektu na dwa sposoby:

   i. na podstawie danych przekazanych do Platformy w drodze integracji z systemu lokalnego po stronie Partnera,
   ii. na wniosek, po dokonaniu zgłoszenia w systemie NCR, jeśli nie jest to możliwe w sposób, o jakim mowa w pkt 5.2) lit. a powyżej,

3) Konta Pracowników Partnera Projektu, którym uprawnienia nadawane są w sposób, o którym mowa w pkt 5.2) lit. a) powyżej, muszą obejmować zakres danych:
   - imię,
   - nazwisko,
   - e-mail
   - nazwę użytkownika
   - część pierwsza kodu resortowego
   - wskazanie ról użytkownika

4) W przypadku Pracowników Partnera Projektu, wykonujących zawód, z którym wiąże się posiadanie numeru prawa wykonywania zawodu dane, o których mowa w pkt 5.3 powyżej muszą obejmować dodatkowo numer prawa wykonywania zawodu.
5) Podmiot Utrzymujący Platformę co najmniej jeden raz na trzy miesiące albo na wniosek Podmiotu Zarządzającego Platforma dokonuje przeglądu uprawnień w zakresie zgodności z danymi, o których mowa w pkt 5.3 i 5.4 powyżej.
6) Konta Pracowników Partnera Projektu niespełniające zakresu danych, o którym mowa w pkt 5.3 i 5.4 powyżej są blokowane przez Podmiot Zarządzający Platform.

7) W przypadku zablokowania konta z przyczyn wskazanych w pkt 5.6 powyżej, Podmiot Utrzymujący Platformę przekazuje o tym informację do Podmiotu Zarządzającego Platformą. Podmiot Zarządzający Platformą przekazuje informację o zablokowanych kontach do Partnera Projektu celem weryfikacji i ewentualnego uzupełnienia danych.
8) Po uzupełnienia danych, o których mowa pkt 5.7 Partnera Projektu występuje z wnioskiem w systemie NCR do Podmiotu Utrzymującego Platformę o odblokowanie uprawnień.

9) Przyznanie uprawnień Pracownikom Partnera Projektu w sposób, o którym mowa w pkt 5.2 lit b powyżej następuje po weryfikacji zgłoszenia wniosku w systemie NCR zawierającego: imię, nazwisko, adres mailowy, numer telefonu oraz wnioskowany zakres dostępu. Wniosek w obszarze formalnym weryfikowany jest przez Podmiot Utrzymujący Platformę. Ponowną weryfikację co do możliwości nadania uprawnień, pod kątem formalnym, tj. weryfikacji wniosku danego Partnera dokonuje Podmiot Zarządzający i na jej podstawie zatwierdza wniosek. Jego realizacją zajmuje się Podmiot Utrzymujący Platformę.
10) Wniosek o dostęp dla Użytkowników ze strony Partnera Projektu, składany w trybie, o którym mowa w pkt 2 lit. 2 powyżej, powinien być zgłoszony w systemie NCR przez osoby odpowiedzialne za kontakt w ramach Projektu. W szczególnych wypadkach dopuszcza się pozyskanie zbiorczej listy kont do wytworzenia od osoby decyzyjnej w zakresie IT ze strony Partnera Projektu (inicjalne wytworzenie kont). O każdej zmianie w zakresie dostępu użytkowników ze strony Partnera Projektu, Partner jest zobowiązany poinformować Podmiot Zarządzający i Podmiot utrzymujący Platformę poprzez system NCR. Nadawanie, zmiana bądź wycofanie uprawnień jest realizowane przez pracowników Podmiotu utrzymującego Platformę po zatwierdzeniu takiego wniosku przez Podmiot Zarządzający, zgodnie z poniższym schematem postępowania:
    a) osoba decyzyjna w zakresie IT ze strony Partnera Projektu występuje do Podmiotu Zarządzającego o nadanie dostępu dla Użytkowników będących personelem Partnera Projektu,
    b) na podstawie postanowień Umowy pomiędzy Partnerami Projektu a Właścicielem Platformy, Osoba upoważniona ze strony Partnera Projektu ustala niezbędny zakres uprawnień dla poszczególnych Użytkowników będących personelem Partnera Projektu,
    c) Podmiot Zarządzający weryfikuje formalnie otrzymany wniosek (tj. poprzez kontakt z Partnerem i potwierdzeniem potrzeby nadania uprawnień) i przekazuje go do realizacji do Podmiotu Utrzymującego Platformę.
    d) Podmiot Utrzymujący Platformę tworzy konta dostępowe zgodnie z zapotrzebowaniem i przekazanymi danymi identyfikacyjnymi. Wytworzone dane dostępowe przekazywane są zainteresowanym użytkownikom w sposób bezpieczny (np. login i hasło dostępowe w zaszyfrowanej paczce ZIP, a hasło do Paczki – poprzez SMS, bezpośrednio do zainteresowanego, na numer telefonu podany w formacie zgłoszenia opisanym w pkt. 5.9) powyżej).
    e) Osoba upoważniona ze strony Partnera Projektu występuje o nadanie, zmianę bądź wycofanie uprawnień do systemów Platformy, zgodnie z opisanymi powyżej krokami,
    f) Podmiot Zarządzający zleca Podmiotowi Utrzymującemu Platformę nadanie, modyfikację bądź wycofanie uprawnień zgodnie ze składanymi wnioskami; w przypadku rejestracji nowego Użytkownika nadawany jest unikalny identyfikator oraz ustawiane jest Hasło Tymczasowe, niezbędne do pierwszego logowania w Systemie. Hasło przekazywane jest bezpiecznym kanałem komunikacji przez Podmiot utrzymujący Platformę.
    g) po nadaniu, zmianie, wycofaniu uprawnień w określonych systemach informatycznych, Podmiot Utrzymujący Platformę informuje Partnera Projektu o wdrożonych zmianach za pośrednictwem Osoby upoważnionej ze strony Partnera Projektu.
11) W przypadku zakończenia przez Partnera Projektu współpracy z pracownikiem/współpracownikiem Partner Projektu bezzwłocznie:
    - składa wniosek o odebranie dostępu dla Pracownika, któremu nadano uprawnienia w sposób określony w pkt 5.2 lit. b)poprzez system NCR. O ile wniosek nie posiada błędów formalnych, ani technicznych, Podmiot Zarządzający akceptuje wniosek i przekazuje go do realizacji do Podmiotu

utrzymującego. Brak zgłoszenia zakończenia współpracy przenosi wszelką odpowiedzialność za aktywność danego Użytkownika na Partnera Projektu.
– odbiera Pracownikowi uprawnienia w systemie dziedzinowym HIS

12) Dostęp do środowiska teleinformatycznego Platformy jest odbierany niezwłocznie w następujących przypadkach:
   a) **Partnerowi Projektu** - jeśli dalszy dostęp do środowiska teleinformatycznego nie jest niezbędny Partnerowi do realizacji umowy głównej o Partnerstwie w Projekcie MSIM, bądź umowy eksploatacji,
   b) **Partnerowi Projektu** - w wyniku stwierdzenia rażących nieprawidłowości i niezgodności podczas audytu bezpieczeństwa przeprowadzonego przez Podmiot Zarządzający u Partnera Projektu,
   c) **Pracownikowi / współpracownikowi Partnera Projektu** – niezwłocznie w przypadku zgłoszenia przez Partnera Projektu faktu rozwiązania umowy z danym pracownikiem ze skutkiem natychmiastowym, bądź w przypadku zakończenia pracy na innej podstawie.

6 Metody i środki uwierzytelniania

1) Dostęp do środowiska teleinformatycznego Platformy MSIM może mieć wyłącznie Użytkownik po podaniu identyfikatora (loginu) i poprawnego hasła. Hasła dostępu do systemu informatycznego (z wyjątkiem hasła startowego) tworzone są przez Użytkownika i stanowią tajemnicę znaną wyłącznie danemu Użytkownikowi. Tworząc hasła dostępowe należy kierować się następującymi wymaganiami:

   a) minimalna długość hasła – 12 znaków,
   b) złożoność hasła – hasło powinno zawierać przynajmniej trzy z czterech opisanych kategorii znaków; tj. dużą literę, małą literę, cyfrę lub znak specjalny (np. !@#) – o ile system informatyczny na to pozwala,
   c) w przypadku systemów informatycznych, które nie wymuszają automatycznie cyklicznej zmiany hasła, obowiązkiem Użytkownika jest zmiana hasła minimum co 90 dni.

2) Zabrania się tworzenia haseł na podstawie:
   a) cech i informacji związanych z użytkownikiem (np. m.in. dat urodzenia, imion, nazwisk, numerów telefonów, przezwisk zwierząt),
   b) sekwencji klawiszy klawiatur (np. qwerty, 12qwaszx),
   c) identyfikatora Użytkownika w jakiejkolwiek formie,
   d) ogólnie dostępnych informacji o Użytkowniku (np. numer telefonu, numer rejestracyjny samochodu itp.)
   e) nazw miesięcy, pór roku, nazw własnych Partnera Projektu czy charakterystycznych dla niego skrótowców (np. $ierpien2023, czerwiec2021).

3) Ponadto zabrania się:
   a) przechowywania haseł w formie jawnej w żadnej postaci elektronicznej lub tradycyjnej, w szczególności w miejscach, gdzie może dojść do nieautoryzowanego dostępu,
   b) wpisywania haseł „na stałe” (np. w telefonie komórkowym, przeglądarkach www). Z zasady tej wyłączone są hasła interfejsów API wykorzystywane w zautomatyzowanych skryptach bądź kodzie źródłowym,
   c) wykorzystywania domyślnych („fabrycznych”) haseł dla ww. urządzeń,
   d) używania tych samych haseł w różnych systemach operacyjnych i aplikacjach.

4) Pierwsze hasło do systemów informatycznych związanych z działaniem Platformy (innych niż Portal Pacjenta), zwane startowym, tworzone jest przez Podmiot Utrzymujący Platformę. Hasło startowe, należy przekazać w formie bezpiecznej, np. z zastosowaniem jednej poniżej proponowanych metod:
   a) Użytkownikowi osobiście po weryfikacji tożsamości – w tym celu Użytkownik zobowiązany jest okazać urzędowy dokument ze zdjęciem pozwalający na jego identyfikację,

b) przez wiadomość tekstową SMS – jeśli we wniosku o nadanie uprawnień Użytkownik wpisał swój służbowy bądź prywatny numer telefonu komórkowego,
c) Osobie upoważnionej wskazanej ze strony Partnera Projektu – w przypadku gdy Partner wnioskuje o dostęp do Platformy po raz pierwszy.

5) Kolejne hasła do systemu informatycznego są zmieniane przez Użytkownika (z wyłączeniem tymczasowej zmiany hasła zgłoszonej poprzez system NCR na żądanie Użytkownika, w przypadku zapomnienia hasła, o ile dany system nie umożliwia samodzielnego jego odzyskania). Hasła powinny pozostać poufne i nawet po ich wygaśnięciu nie mogą być udostępniane innym osobom, w tym Administratorom IT. W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło Użytkownika w sposób nieuprawniony, Użytkownik zobowiązany jest do natychmiastowej zmiany hasła i zgłoszenia tego faktu jako incydentu bezpieczeństwa – zgodnie z rozdziałem 10 niniejszej Polityki.

7 Minimalne wymagania w zakresie bezpieczeństwa

1) Platforma MSIM została zaprojektowana w środowisku rozproszonym. W celu zapewnienia ciągłości dostępu do informacji udostępnianych wymaga się, by Partnerzy Projektu, z których systemów wczytywane są do Platformy informacje o zdarzeniach medycznych spełniali minimalne wymagania techniczne jak poniżej:
   a) Partnerzy stosują łącze Internetowe redundantne, symetryczne o przepustowości minimum 100Mbit.
   b) Partnerzy mają możliwość wydzielania dedykowanego pasma z i do Platformy MSIM dla udostępnianych usług wraz z priorytetyzacją ruchu. Komunikacja z i do Platformy MSIM musi mieć przypisany wyższy priorytet, niż dowolne inne kategorie ruchu prywatnego użytkowników, tj. niezwiązanego z realizacją świadczeń medycznych lub pozostałą działalnością podmiotu leczniczego.
   c) Musi być zapewniona wysoka dostępność komponentów biorących udział w wymianie danych z Platformą MSIM, w tym zalecane jest zdublowanie elementów infrastruktury techniczno-systemowej.
   d) Urządzenia sieciowe biorące udział w wymianie i komunikacji z Platformą MSIM, w szczególności zapory ogniowe i przełączniki sieciowe, są redundantne.
   e) Udostępnianie danych i wymiana danych realizowana jest tylko w ramach zestawionego szyfrowanego protokołu TLS w wersji minimum 1.2.
   f) Stosuje się zestawienia połączenia site-to-site VPN z Platformą MSIM zabezpieczonego certyfikatem i hasłem.
   g) Ruch z i do Platformy MSIM jest być filtrowany i poddawany inspekcji.
   h) Wszystko co nie jest dozwolone jest zabronione w ramach komunikacji z Platformą MSIM.
   i) Poszczególne komponenty biorące udział w wymianie danych z Platformą MSIM są umieszczone w wydzielonych strefach, pomiędzy którymi ruch jest filtrowany i wykonywana jest inspekcja.
   j) Przekazywane do repozytorium regionalnego dokumenty podlegają inspekcji antywirusowej.
   k) Zapewniona jest integralność dokumentów poprzez podpis cyfrowy przewidziany przepisami prawa w zakresie podpisywania dokumentacji medycznej.
   l) Każda interakcja komponentów MSIM między sobą oraz z systemami lokalnymi wymaga synchronizacji czasu zgodnie z założeniami profilu IHE CT.
   m) Wymagana się zapewnienia rozliczalności i logowania zdarzeń po stronie Partnera.
   n) Zasoby podlegające wymianie danych muszą podlegać polityce kopii zapasowej.
   o) Systemy lokalne przechowują dane medyczne i dokumenty medyczne przez okres wymagany obowiązującymi przepisami prawa dla każdej z kategorii danych medycznych i dokumentów medycznych.
   p) Uwierzytelnienie systemów pomiędzy Platformą MSIM a Partnerami jest wykonywane przy wykorzystaniu wzajemnego uwierzytelniania (Mutual Authentication). Platforma MSIM jest dostawcą tożsamości.
   q) Usługi udostępniane przez Partnera są możliwe do monitorowania przez Platformę MSIM.

r) Istnieje możliwość udostępniania danych do regionalnego repozytorium poprzez komunikaty realizowane w technologii Web Services. Komunikaty wykorzystują model SOAP w wersji 1.2.
s) Interfejsy realizowane w technologii Web Services korzystają z WS Security na potrzeby przekazywania informacji o uprawnieniach użytkownika zgodnie z profilem IHE XUA.
t) Interfejsy realizowane w technologii Web Services dla transakcji IHE, są zgodne z sekcją ITI TF-2x: Appendix V: Web Services for IHE Transactions.

2) W celu poprawy ciągłości w zakresie dostępności, prócz spełnienia powyższych wymagań rekomendujemy:
   a) Zastosowanie redundantnego łącza Internet w technologii FC, symetrycznego o przepustowości nie gorszej niż 1GB/s, doprowadzonego z dwóch różnych kierunków od dwóch różnych operatorów – celem minimalizacji zakłóceń, a przy użytku codziennym – zrównolegleniu obciążenia;
   b) Odmiejscowienia Zapasowego Centrum Przetwarzania Danych (zapasowa serwerownia posiadająca dane nie starsze niż 12h przynajmniej w innej części budynku)
   c) Wdrożenie oprogramowania klasy EDR, docelowo XDR
   d) Wdrożenia polityki aktualizacji systemów odpowiedniej do Organizacji, uwzględniającej czasy życia wykorzystywanego oprogramowania
   e) oprogramowanie do tworzenia kopii zapasowych pozwalające na łatwe zarządzanie backupem, odtworzenie kopii w prosty sposób z dowolnie zadanego dnia
   f) Partner korzysta z systemów operacyjnych dla serwerów w wersji aktualnej, dla której dostawca oprogramowania zapewnia wsparcie przynajmniej przez kolejnych 3 lat
   g) Testowanie kopii zapasowych nie rzadziej niż co kwartał przy konfiguracji kopii zapasowych – RPO = 4h

3) Partner Projektu musi zapewnić, że zadania realizowane w ramach Platformy MSIM będą zarządzane zgodnie z najlepszymi praktykami określonymi w rozdz. 5.8. normy ISO/IEC 27002:2022 oraz wymaganiami niniejszej Polityki. W szczególności musi zostać zapewnione, aby Partner:
   a) zidentyfikował cele biznesowe przystąpienia do Projektu
   b) zidentyfikował cele w zakresie bezpieczeństwa i ochrony danych osobowych istotne dla niego (jako ADO) związane z uczestnictwem w Projekcie,
   c) zidentyfikował i oszacował ryzyka związane z realizacją udziału w działaniach Platformy,
   d) zdefiniował i zastosował zabezpieczenia adekwatne do zidentyfikowanych ryzyk, jakie był w stanie wdrożyć po stronie swojej infrastruktury,
   e) opracował lub posiada plany ciągłości gwarantujące dostępność danych Pacjentów udostępnianych w ramach Platformy.

4) Partner Projektu powinien posiadać i stosować klasyfikację przesyłanych, przetwarzanych i przechowywanych danych osobowych oraz informacji ważnych z punktu widzenia jego jako Administratora Danych Osobowych (w kontekście wymagania art. 5 pkt 1 lit. c) Rozporządzenia RODO) dla jego działalności. Podczas tworzenia takiego dokumentu pomocnymi mogą być wymagania opisane w rozdz. 5.12 normy PN-ISO/IEC 27002:2022. W ramach działania Platformy proponuje się następującą klasyfikację przetwarzanych danych i posiadanych aktywów:

   a) Poziom poufności "**Publiczne**": Informacje publiczne są dostępne dla ogółu społeczeństwa i nie wymagają żadnych ograniczeń ani zabezpieczeń. Są to informacje ogólnodostępne, które nie są wrażliwe lub luźno związane z działaniem Platformy MSIM. (m. in. Polityki Prywatności, obowiązki informacyjne, deklaracja dostępności WCAG)
   b) Poziom poufności "**Do użytku wewnętrznego**": Informacje wewnętrzne są przeznaczone wyłącznie dla pracowników i osób pośrednio lub bezpośrednio związanych z utrzymaniem, czy zarządzaniem Platformą. Mogą obejmować dane operacyjne, dokumenty wewnętrzne i inne informacje, które nie są przeznaczone dla osób postronnych. (m. in. Instrukcje utrzymania Platformy)

c) Poziom poufności "**Szczególnie chronione**": Informacje ograniczone są bardziej wrażliwe niż informacje wewnętrzne i wymagają większych środków ochrony. Dostęp do tych informacji powinien być udzielany tylko osobom upoważnionym, które mają konkretną potrzebę dostępu związanych z wykonywanymi zadaniami. Informacje sklasyfikowane jako „Szczególnie chronione" mogą obejmować dane osobowe, poufne dane biznesowe, tajemnice handlowe itp. (m. in. Polityki bezpieczeństwa, raporty z testów – nie tylko bezpieczeństwa, architektura rozwiązania Platformy, dane osobowe administratorów systemów dziedzinowych (imię, nazwisko, nr. tel. mail, uprawnienia do zarządzania systemem))
d) Poziom poufności "**Wrażliwe**": Informacje wrażliwe wymagają najwyższych środków ochrony. Dostęp do informacji o Pacjentach i ich zdrowiu, logach systemowych z działania Platformy powinien być ściśle kontrolowany i ograniczony do osób o najwyższych uprawnieniach. Informacje wrażliwe mogą obejmować dokumentację medyczną, dostępy głównego administratora, dane o dostępie do logów zdarzeń itp.

5) Partner Projektu jest zobowiązany do zapewnienia, przy dochowaniu najwyższej staranności, właściwej ochrony udostępnionego środowiska teleinformatycznego Platformy, w szczególności wdrożenia po swej stronie mechanizmów organizacyjno-technicznych gwarantujących:
   a) dostęp do systemów lub zasobów teleinformatycznych wyłącznie dla uprawnionych Użytkowników,
   b) rozliczalność Użytkowników, rozumianą jako możliwość jednoznacznego przypisania działań prowadzonych w systemie lub zasobie do konkretnego Użytkownika.
6) Realizując wymagania, o których mowa w pkt. 5, Partner Projektu zapewni w szczególności:
   a) ochronę wszelkich udostępnionych mu przez Podmiot Zarządzający Platformą urządzeń, komponentów sprzętowych (np. klucze kryptograficzne), kart dostępu fizycznego oraz elementów programowych (np. środowiska ewaluacyjnego) oraz wszelkich informacji (np. loginy i hasła) przed dostępem osób nieuprawnionych,
   b) skuteczne mechanizmy organizacyjne i techniczne uniemożliwiające Użytkownikom:
      i. dokonywanie prób sprawdzania, testowania i omijania zabezpieczeń systemów teleinformatycznych Platformy,
      ii. podejmowanie działań, które pośrednio lub bezpośrednio mogą prowadzić do naruszenia bezpieczeństwa udostępnionych systemów lub zasobów teleinformatycznych.
7) Partner Projektu musi zapewnić bezpieczeństwo informacji przesyłanej do Platformy w związku z realizacją Umowy o Partnerstwie zgodnie wymaganiami określonymi w rozdz. 5.21 normy ISO/IEC 27002:2022. W szczególności musi:
   a) zapewnić ochronę poufności oraz integralności informacji przesyłanej publicznymi kanałami transmisyjnymi, odpowiednio do jej klasy bezpieczeństwa,
   b) zapewnić, że wszystkie osoby mające dostęp do informacji chronionych lub szczególnie chronionych podpisały klauzule poufności,
   c) zapewnić szyfrowanie komunikacji w oparciu o rozwiązania zapewniające poziom bezpieczeństwa, co najmniej równy temu jaki zapewniają protokoły TLS w wersji co najmniej 1.2 lub VPN.
8) Partner Projektu powinien zapewnić bezpieczeństwo wykorzystywanego personelu zgodnie z najlepszymi praktykami określonymi w rozdz. 5.4; 6.3 oraz 6.5 normy ISO/IEC 27002:2022, adekwatnie do zadań realizowanych w ramach Platformy. W szczególności, musi posiadać i realizować udokumentowane polityki zarządzania personelem, które obejmują:
   a) przekazanie własnemu personelowi, realizującemu zadania z wykorzystaniem narzędzi udostępnianych przez Platformę, informacji o wymaganiach bezpieczeństwa współpracy z w ramach Platformy,
   b) wdrożenie programu okresowych szkoleń z zakresu bezpieczeństwa informacji i cyberbezpieczeństwa, a następnie zapewnienie udziału personelu pracującego na systemach związanych z Platformą w tych szkoleniach.
9) Partner Projektu musi zapewnić właściwe użycie aktywów, powierzonych przez Właściciela Platformy bądź Podmiot Zarządzający Platformą, wykorzystywanych w pracach na systemach związanych z

Platformą zgodnie z uznanymi praktykami określonymi w rozdz. 5.10 i 5.11 normy ISO/IEC 27002:2022. W szczególności wymaganym jest aby:

a) użytkownicy tych aktywów posiadali świadomość odnośnie bezpiecznego korzystania z udostępnionych aktywów,
b) po zakończeniu realizacji zleconych zadań użytkownicy zwrócili aktywa lub, w przypadku gdy są to dane, usunęli je w skuteczny sposób.

10) Partner Projektu powinien zapewnić ochronę systemów Platformy przed działaniem szkodliwego oprogramowania zgodnie z najlepszymi praktykami określonymi w rozdz. 8.7 normy ISO/IEC 27002:2022. W szczególności musi posiadać:
    a) zabezpieczenia wykrywające, zapobiegające i odtwarzające, które służą ochronie przed szkodliwym oprogramowaniem
    b) dbać o świadomość pracowników w kontekście stosowania aktualnych wersji takich zabezpieczeń.
11) Wszelkie oprogramowanie wykorzystywane w ramach realizacji przedmiotu Umowy o Partnerstwie musi być użytkowane z poszanowaniem praw własności intelektualnej, w szczególności zgodnie z ustawą o prawie autorskim i prawach pokrewnych.

8 Kryptografia

1) W celu ochrony poufności przesyłanych oraz przechowywanych danych stosuje się zabezpieczenia kryptograficzne. W szczególności Partnerzy stosują następujące zabezpieczenia kryptograficzne:
    a) na dyskach twardych komputerów przenośnych,
    b) na pamięciach wymiennych typu pendrive, dysk zewnętrzny itp.
    c) na nośnikach kopii zapasowych przechowywanych poza obszarem kolokacji Platformy,
    d) tunelach VPN,
    e) w korespondencji elektronicznej, w trakcie przesyłania danych objętych ochroną, w szczególności danych osobowych (np. stosując szyfrowanie paczek ZIP; 7Z czy szyfrując wewnętrznie pliki DOCX; XLSX itd.).
2) Zakres stosowanych rozwiązań kryptograficznych powinien obejmować minimum dane znajdujące się na nośnikach, które objęte są ochroną ze względu na wymagania utrzymania odpowiedniego poziomu poufności. Rozwiązania kryptograficzne powinny wykorzystywać algorytm AES (lub mocniejszy) o długości klucza minimum 256 bit.

9 Bezpieczeństwo środowisk związanych z Platformą

9.1 Realizacja zgłoszeń dotyczących dokumentacji pacjenta

1. Platforma posiada dedykowany moduł obsługi zgłoszeń wspierający obsługę zgłoszeń związanych z wyświetlaniem dokumentacji medycznej.
2. Zgłoszenia może dokonać Lekarz, bądź bezpośrednio Pacjent, którego dane są wyświetlane niepoprawnie w platformie.
3. Zgłoszenia dzieli się na dwa podtypy:
    a. Zgłoszenie problemu z brakiem dokumentacji medycznej – gdzie wskazuje się brak danego dokumentu, gdy właściwa osoba ma wiedzę o zdarzeniu medycznym i wygenerowaniu dokumentacji z danego zdarzenia.
    b. Zgłoszenie problemu z zawartością dokumentacji medycznej – gdy właściwa osoba nie jest w stanie odczytać zawartości dokumentu medycznego, bądź gdy zawiera on dane niekompletne lub niewłaściwe.
4. System każdorazowo wymaga uzupełnienia pól opisowych zgłoszenia, umożliwiając szczegółowe określenie nieprawidłowości oraz/lub identyfikację zdarzenia towarzyszącego powstaniu dokumentacji. Wskutek zastosowanych mechanizmów zarządzania uprawnieniami pacjenci nie są uprawnieni do zgłaszania błędów dotyczących dowolnych dokumentów medycznych. Ich uprawnienia

ograniczają się wyłącznie do dokumentacji, do której posiadają nadane uprawnienia dostępu lub o której istnieniu posiadają uzasadnioną wiedzę.

5. Zgłaszane błędy mogą w szczególności dotyczyć występowania duplikatów tj. zwielokrotnionych rekordów pacjenta MPI. Zarządzanie duplikatami na poziomie lokalnym powinno być realizowane zgodnie z wewnętrznymi procedurami przez Partnera Projektu. W przypadku duplikatów na poziomie regionalnym dokumentacja medyczna jest prezentowana zbiorczo dla odpowiedniego pacjenta.
6. Kolejka zgłoszeń związanych z dokumentacją medyczną prezentowana jest w Portalu Administratora i pozwala na pełną obsługę zgłoszenia. System pozwala na przypisanie osoby obsługującej zgłoszenie, co zapewnia rozliczalność działań z dokładnością do czasu obsługi zgłoszenia przez podmioty zaangażowane.
7. Do podmiotów, które są zaangażowane w obsługę zgłoszenia należą w szczególności:
    a. Podmiot Zarządzający,
    b. Podmiot Utrzymujący Platformę,
    c. Partner Projektu.
8. Status realizacji zgłoszeń w kolejce monitoruje Podmiot Zarządzający (MPP) jako posiadający uprawnienia administratora regionalnego. Realizacja zgłoszeń prowadzona jest zgodnie z bieżącymi potrzebami.

10 Procedura obsługi wniosków osób, których dane dotyczą na Platformie MSIM

1. Szczegółowe zasady komunikacji pomiędzy Administratorami danych, Właścicielem Platformy, Podmiotem utrzymującym Platformę i podmiotami danych w zakresie zawiadamiania, przepływu danych i współpracy w zakresie realizacji praw osób reguluje niniejsza procedura.
2. Z perspektywy Podmiotu Zarządzającego proces obsługi wniosków wynikających z praw, wskazanych w np. 15-22 RODO składa się z następujących kroków:

a) Osoba (podmiot danych), której dane są przetwarzane w ramach Platformy zgłasza żądanie do Podmiotu Zarządzającego. Żądanie powinno mieć formę udokumentowaną (postać mailową bądź listowną) i dostatecznie identyfikuje podmiot danych, którego dotyczy wniosek (tj. zawiera m. in. np. Imię, nazwisko, PESEL, adres zamieszkania, bądź wskazuje w jakich podmiotach dokonywano leczenia), dane kontaktowe, opis żądania i podstawę jego wystosowania. Jeżeli Podmiot Zarządzający nie ma możliwości weryfikacji wnioskującego, wzywa go do osobistego stawiennictwa w siedzibie Podmiotu Zarządzającego, celem obsługi wniosku;
b) Jeżeli wniosek taki wpłynie do innych podmiotów współpracujących na rzecz działania Platformy, to o ile ten podmiot nie jest właściwym ADO dla wniosku, przekazuje go do obsłużenia Podmiotowi Zarządzającemu, w formie mailowej;
c) Podmiot Zarządzający posiada wyznaczoną osobę / osoby odpowiedzialne za obsługę tego typu wniosku, która realizuje poniższe kroki:
    i. Podmiot Zarządzający za pomocą dostępnych środków (np. min. kontakt z PUP) ustala, z jakich systemów Partnerów pochodzą dane tejże osoby;
    ii. Po ustaleniu systemów Podmiot Zarządzający przekazuje żądanie osoby do odpowiednich ADO – właściwych względem pochodzenia danych w systemie.
    iii. Podmiot Zarządzający informuje osobę o przekazaniu żądania do poszczególnych ADO od których powziął dane, wraz z informacją, że dalsze kroki obsługi tego wniosku realizowane będą przez odpowiednich ADO;
    iv. Podmiot Zarządzający odpowiada w sposób samodzielny (wnioski gdzie ADO jest UMWM) chyba, że UMWM zadecyduje inaczej.
    v. ADO właściwi dla danych obsługują wnioski zgodnie z odpowiednimi dla wniosków, wewnętrznie przyjętymi regulacjami Partnera, i prowadzą w tej sprawie komunikacje z Podmiotem danych. Po zakończeniu obsługi wniosku, w terminie nie dłuższym niż 2 dni robocze, Administrator właściwy

dla sprawy informuje w formie mailowej Podmiot Zarządzający o zakończeniu obsługi wniosku, o ile wniosek ten dotyczył działania Platformy.

3. Szczegółowe kroki wymagane do poprawnej realizacji wniosku zaprezentowano w modelu BPMN procesu obsługi wniosków, dołączonego do niniejszego dokumentu.

11 Zarządzanie incydentami

1) Zaleca się by Partner Projektu zapewnił identyfikowanie i obsługę incydentów bezpieczeństwa zgodnie z najlepszymi praktykami określonymi w normie ISO/IEC 27002:2022 rozdz. 5.24 (tj. Partnerzy powinni zaplanować i przygotować się do zarządzania incydentami związanymi z bezpieczeństwem informacji w ramach własnej działalności, poprzez określenie ustanawianie i komunikowanie ról i odpowiedzialności w procesach zarzadzania incydentami bezpieczeństwa informacji); 5.25; (tj. Partnerzy powinni być w stanie ocenić zdarzenia związane z bezpieczeństwem informacji i decydować czy sklasyfikować je jako incydenty związane z bezpieczeństwem informacji, czy też nie. Klasyfikacja ta powinna dotyczyć systemów i zdarzeń zachodzących w środowisku Partnera.); 5.26 normy ISO/IEC 27002:2022 (tj. reakcja Partnera projektu na incydenty związane z bezpieczeństwem informacji powinna być zgodna z udokumentowanymi procedurami).
2) Partner w szczególności zobowiązany jest do niezwłocznego zgłaszania wszelkich zauważonych zdarzeń, które noszą znamiona lub są incydentami bezpieczeństwa lub ochrony danych osobowych, udzielania wszelkich niezbędnych informacji oraz wsparcia pracowników Podmiotu Zarządzającego zaangażowanych w proces obsługi incydentu bezpieczeństwa. W przypadku zaistnienia incydentu bezpieczeństwa Partner Projektu musi podjąć wszelkie niezbędne środki, aby zminimalizować wpływ incydentu na działanie elementów Platformy. Zaleca się by Partner Projektu posiadał odpowiednie procedury umożliwiające gromadzenie wszelkich dowodów związanych z zaistnieniem incydentu bezpieczeństwa, tj. powinien dla systemów własnych opracować, wdrożyć i stosować procedury na wypadek gromadzenia, pozyskiwania i zabezpieczania dowodów w zakresie bezpieczeństwa informacji zgodnie z wymaganiami rozdz. 5.28 normy ISO/IEC 27002:2022.
3) Użytkownik Portalu Pracownika Medycznego zobowiązany jest zawiadomić odpowiedniego Partnera Projektu o pojawiających się komunikatach wskazujących na wystąpienie zagrożenia spowodowanego szkodliwym oprogramowaniem. Partner Projektu dokonuje poszerzonego skanowania stanowiska komputerowego swojego pracownika. W przypadku wykrycia wirusów komputerowych na danym stanowisku, sprawdzane są również wszystkie nośniki posiadane przez użytkownika. Sytuacja taka odnotowywana jest w rejestrze incydentów. Dalsze kroki powinny być zbieżne z procedurami wewnętrznymi danego Partnera.
4) Wszelkie zdarzenia wskazujące na naruszenie lub możliwość naruszenia zasad bezpieczeństwa informacji należy niezwłocznie zgłaszać: poprzez wiadomość e-mail na adres: incydent@mpp.krakow.pl.
5) W sytuacjach pilnych wszelkie zdarzenia należy telefonicznie zgłaszać do Podmiotu Zarządzającego pod numerem: (+48) 573 217 545
6) Jeżeli naruszenie w jednoznaczny sposób dotyczy bezpieczeństwa przetwarzania danych osobowych, Partner Projektu zobowiązany jest do bezpośredniego powiadomienia Podmiotu Zarządzającego o tym fakcie. Zgłoszenia należy dokonać za pośrednictwem poczty elektronicznej, za potwierdzeniem odczytania, na adres: iod@mpp.krakow.pl, z tematem wiadomości „Naruszenie ochrony danych”.
7) Zgłoszenie incydentu bądź podejrzenia incydentu musi zawierać jak najbardziej szczegółowe informacje, m.in.:
   a) imię i nazwisko zgłaszającego, dane kontaktowe (e-mail, telefon kontaktowy),
   b) nazwę podmiotu Partnera Projektu,
   c) miejsce, data i czas wystąpienia zdarzenia,
   d) szczegółowy opis zdarzenia:
      i. jakiego systemu, bądź Portalu dotyczy zgłoszenie,
      ii. opis incydentu (opisowo),

iii. ewentualny wpływ incydentu na funkcjonowanie systemu / Portalu, w którym on wystąpił, oraz w systemach z nim powiązanych i zależnych,
iv. wstępne skutki i oszacowanie szkód (jeśli doszło do materializacji takowych),
v. czy czynnik wywołujący incydent (na przykład intruz albo złośliwe oprogramowanie) został zidentyfikowany i czy jego aktywność nadal trwa,
vi. zrzuty ekranu, komunikaty oraz logi systemowe w załącznikach (jeśli istnieje możliwość udokumentowania),

8) Osoba, która zgłosiła zdarzenie, posiadające znamiona incydentu nie powinna podejmować żadnych działań na własną rękę, jednak w miarę możliwości powinna zabezpieczyć materiał dowodowy, np. wykonując zdjęcie ekranu, co do którego zaistniało podejrzenie, że jego działanie odbiega od normy. Jeśli zdarzenie ma miejsce w infrastrukturze zarządzanej przez Partnera Projektu, upoważnione osoby ze strony Partnera Projektu (np. m.in. pracownicy działu IT po stronie Partnera Projektu, specjaliści ds. bezpieczeństwa wewnętrznego) zabezpieczają ślady (np. logi systemowe, zrzuty ekranu, zrzuty pamięci) z takiego zdarzenia.

9) Podmiot Zarządzający zastrzega sobie prawo do zbierania i zabezpieczania wszelkich dowodów wskazujących na wystąpienie i powstanie skutków incydentu bezpieczeństwa, w szczególności prawo do wystąpienia do Partnera Projektu z pisemnym żądaniem niezwłocznego włączenia się w obsługę incydentu bezpieczeństwa, w tym niezwłocznego podania wszelkich niezbędnych informacji w zakresie badanego incydentu bezpieczeństwa. Podmiot Zarządzający jest zobowiązany niezwłocznie powiadomić Partnera Projektu, wskazując kto z ramienia Podmiotu Zarządzającego odpowiedzialny jest za kontakt w sprawie.
10) Szczegółowy tryb postępowania w przypadku incydentu, regulują wewnętrzne procedury w zakresie Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych. Każdorazowo, po zamknięciu incydentu, osoba obsługująca incydent ze strony Podmiotu Zarządzającego, zgodnie z procedurami wewnętrznymi sporządza Raport z incydentu oraz wydaje rekomendacje w zakresie działań zmierzających do zmniejszenia ryzyka powtórzenia incydentu w przyszłości, które przedstawiane są Partnerowi Projektu wraz z potencjalnymi rekomendacjami wdrożenia wymaganych środków bezpieczeństwa.
11) Administrator Danych Osobowych właściwy dla danych, których dotyczyło naruszenie zgodnie z przepisami dokonuje zgłoszenia do PUODO, organizacji lub osoby, której naruszenie dotyczy.
12) W przypadku wystąpienia naruszenia ochrony danych osobowych dotyczącego danych przetwarzanych w ramach Platformy, Podmiot Zarządzający wraz z Podmiotem utrzymującym Platformę współpracują z Właścicielem Platformy oraz Partnerami Projektu i pomagają im w wypełnianiu obowiązków wynikających z art. 33 i 34 RODO, z uwzględnieniem charakteru przetwarzania i informacji, którymi dysponuje Podmiot Zarządzający wraz z Podmiotem utrzymującym Platformę.

12 Uprawnienia audytowe Właściciela Platformy

1) Właściciel Platformy zastrzega sobie prawo do przeprowadzenia audytów zgodności i bezpieczeństwa zastosowanych przez Partnera Projektu rozwiązań organizacyjno-technicznych, które mogą być przeprowadzone przez Podmiot Zarządzający na zlecenie Właściciela. Audyty takie dotyczyć będą stosowania zaimplementowanych mechanizmów bezpieczeństwa z obowiązującym prawem i niniejszą Polityką oraz sposobu korzystania przez personel Partnera Projektu z udostępnionych im systemów lub zasobów teleinformatycznych Platformy. Partner Projektu nie może odmówić przeprowadzenia audytu. Audyt może być przeprowadzony w dni robocze, w godz. 9.00 – 16.00, w terminie ustalonym z Podmiotem Zarządzającym i przekazanym pisemnie ustaleniem do wiadomości Partnera Projektu, z co najmniej 14-dniowym wyprzedzeniem. Z przyczyn obiektywnych, przedłożonych Podmiotowi Zarządzającemu Platformą, Partner Projektu może zgłosić propozycję przesunięcia terminu audytu, lecz powinno to nastąpić nie później niż na 7 dni przed datą audytu.

2) Partner Projektu musi zapewnić Podmiotowi Zarządzającemu możliwość przeprowadzenia audytów bezpieczeństwa w zakresie danych wymienianych w ramach Platformy, bądź własnych środowisk informatycznych wykorzystywanych do współpracy z Podmiotem Zarządzającym.
3) Partner Projektu zobowiązany jest do umożliwienia przeprowadzenia audytu w szczególności poprzez:
   a) umożliwienie osobom audytującym wstępu do pomieszczeń Partnera Projektu, w których jest wykonywana działalność związana z Umową,
   b) zapewnienie osobom audytującym dostępu do wszelkich wymaganych informacji, urządzeń oraz systemów teleinformatycznych wykorzystywanych do realizacji Umowy oraz personelu Partnera Projektu i dokumentów w zakresie wynikającym z Umowy,
   c) udzielanie osobom audytującym przez osoby zaangażowane w realizację Umowy ze strony Partnera Projektu wyjaśnień w żądanej formie - pisemnej lub ustnej w zakresie wynikającym z realizacji przedmiotu Umowy.
4) Zgodnie z wymaganiami normy PN-EN ISO 19011:2018-08 wyniki audytu powinny być omówione z przedstawicielami Partnera Projektu. Z audytu musi zostać sporządzony udokumentowany raport, oraz przedstawione karty niezgodności - w przypadku zidentyfikowania niezgodności. W przypadku stwierdzenia uchybień w zakresie objętym audytem, Właściciel Platformy poprzez Podmiot Zarządzający Platformą ma prawo wezwać Partnera Projektu do podjęcia działań w celu ich usunięcia w wyznaczonym terminie. Brak usunięcia uchybień w wyznaczonym terminie, może stanowić podstawę do wypowiedzenia Umowy Partnerskiej / Umowy Eksploatacji.

13 Udostępnianie dokumentacji

1) Udostępnienie dokumentacji innej osoby następuje w wyniku przekazania przez pacjenta zgody w danym szpitalu. Udzielenie zgody procedowane jest na zasadach określonych wewnętrznie przez szpital.
2) Dla potrzeb spełnienia wymogów zgodności z art. 27 ust. 4 przyjmujemy następujące rozumienie danych w rejestrze:
   a) imię (imiona) i nazwisko pacjenta, którego dotyczy dokumentacja medyczna - zgodne z zapisami w MPI MSIM;
   b) sposób udostępnienia dokumentacji medycznej – poprzez Platformę MSIM;
   c) zakres udostępnionej dokumentacji medycznej; - zakres dokumentacji dostępnej w MSIM (ze wskazanymi datami);
   d) imię (imiona) i nazwisko osoby innej niż pacjent, której została udostępniona dokumentacja medyczna, a w przypadkach, o których mowa w art. 26 ust. 3 i 4, także nazwę uprawnionego organu lub podmiotu;
   e) imię (imiona) i nazwisko oraz podpis osoby, która udostępniła dokumentację medyczną; - osoba posiadająca uprawnienia u Partnera (w HIS), która dokonuje uruchomienia funkcjonalności umożliwiającej udostępnienie;
   f) datę udostępnienia dokumentacji medycznej - data udostępnienia z upoważnienia (zgody pacjenta składanej w szpitalu).

14 Postanowienia końcowe

1) Za nadzór nad przestrzeganiem postanowień niniejszej Polityki odpowiada:
   a) ze strony Partnera Projektu, uprawniony przedstawiciel Partnera Projektu,
   b) ze strony Właściciela Platformy – Podmiot Zarządzający Platformą we współpracy technicznej z Podmiotem Utrzymującym Platformę.

2) Naruszając zapisy niniejszej Polityki, Partner Projektu może podlegać sankcjom karnym, cywilnym oraz wynikającym z przepisów art. 107 i art. 108 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

Załącznik nr 1: Wzór oświadczenia

OŚWIADCZENIE

Oświadczam, że zapoznałem/am się z Polityką Bezpieczeństwa dla Partnerów oraz z przepisami powszechnie obowiązującymi dotyczącymi ochrony danych osobowych, w tym z RODO, a także przekazanymi wymaganiami bezpieczeństwa w ramach działania Platformy MSIM i zobowiązuję się do przestrzegania zasad przetwarzania danych osobowych określonych w tych dokumentach.

Zobowiązuję się do zachowania w tajemnicy przetwarzanych danych osobowych, z którymi zapoznałem/am się oraz sposobów ich zabezpieczania, zarówno w okresie trwania umowy jak również po ustaniu stosunku prawnego.

Zobowiązuję się do właściwego zabezpieczania danych osobowych, w szczególności przed nieuprawnionym dostępem, zmianą, utratą, uszkodzeniem lub zniszczeniem.

Zobowiązuję się do zgłaszania wszelkich naruszeń ochrony danych osobowych właściwemu Inspektorowi Ochrony Danych.

_____

Czytelny podpis osoby składającej oświadczenie