Załącznik nr 1 do wniosku o dofinansowanie

nabór FELD.01.04-IP.02-001/25

**……………………………………….**

Miejscowość, data

**…………………………………………………………**

Nazwa i adres wnioskodawcy

**ZAPEWNIENIE ROZWIĄZAŃ**

|  |  |
| --- | --- |
| 1. **ZASTOSOWANE ROZWIĄZĄŃ W OBSZARZE:** | |
| **A.1 GROMADZENIE I WYMIANA DANYCH MEDYCZNYCH**  *Należy przedstawić informacje jakie rozwiązania zastosowano w projekcie. Jeżeli projekt nie dotyczy danego obszaru wpisz ND* | |
| 1.zlecenia procedur medycznych (badań, konsultacji, podania leków) oraz przekazanie wyników tych procedur personelowi medycznemu będą w całości realizowane w systemach teleinformatycznych (np. w systemie szpitalnym HIS, laboratoryjnym LIS, radiologicznym RIS, farmaceutycznym PIS, kardiologicznym CIS) |  |
| 2.ponad 90% obrazów medycznych (DICOM, nie-DICOM) oraz wyników badań laboratoryjnych będzie przechowywanych w systemie teleinformatycznym, a dane te będą powiązane z danymi pacjenta oraz zdarzeniami medycznymi, w ramach których były realizowane |  |
| 3.ponad 90% wyników badań laboratoryjnych (m.in. biochemia kliniczna, mikrobiologia, badania molekularne) będzie przechowywanych w formie  ustrukturyzowanych  danych, które można wykorzystać w ramach analiz niezbędnych do podejmowania decyzji klinicznych |  |
| 4.w procesie zarządzania podawaniem leków będą wykorzystywane interaktywne alerty, zapewniające bezpieczeństwo podawania leków (np. zduplikowane zlecenia, interakcje leków, nieprawidłowe dawki). Podmioty wykonujące działalność leczniczą będą gromadzić dane o wszystkich produktach leczniczych podanych pacjentowi w trakcie udzielania świadczeń wraz z dawką i czasem podania |  |
| 5.podmiot wykonujący działalność leczniczą będzie posiadał system informatyczny zgodny z wymaganiami art. 8b ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (dalej: USIOZ). Weryfikacji podlegać będzie m.in. czy podmiot udzielający świadczeń zdrowotnych:  a) gromadził jednostkowe dane medyczne,  b) tworzył EDM;  c) udostępniał EDM,  d) udostępniał obrazy medyczne w formacie plików DICOM;  e) identyfikował się i wymieniał jednostkowe dane medyczne;  f) jest zintegrowany z innymi systemami e-zdrowia  zgodnie z Polską Implementacją Krajową HL7 CDA, profilami IHE,  standardami, o których mowa w art. 8d USIOZ, zamieszczonymi w  Biuletynie Informacji Publicznej ministra właściwego do spraw zdrowia i na stronie www.ezdrowie.gov.pl oraz zgodnie z rekomendacjami Rady ds. Interoperacyjności |  |
| 6.system teleinformatyczny usługodawcy będzie umożliwiać (upoważnionym pracownikom medycznym) pobranie EDM pacjenta wytworzonej w innych podmiotach wykonujących działalność leczniczą |  |
| **A.2 ANALITYKA MEDYCZNA**  *Należy przedstawić informacje jakie rozwiązania zastosowano w projekcie. Jeżeli projekt nie dotyczy danego obszaru wpisz ND* | |
| 1.zostaną określone zasady oraz procedury dotyczące przepływu danych medycznych w podmiocie wykonującym działalność leczniczą, w tym m.in. zasady skanowania danych przy łóżku pacjenta (skanowanie z wykorzystaniem czytników kodów kreskowych, QR) |  |
| 2.podmiot wykonujący działalność leczniczą będzie agregował raporty z wyników dotyczących efektywności finansowej oraz działalności podstawowej (medycznej) w celu ich wykorzystania do zarządzania jakością i efektywnością. Raporty będą przeznaczone dla personelu medycznego monitującego skuteczność leczenia pacjentów, kadry zarządzającej podmiotem leczniczym oraz dla podmiotów nadzorujących działanie podmiotów podległych. |  |
| **A.3 CYBERBEZPIECZEŃSTWO**  Należy przedstawić informacje czy zostanie zapewniony adekwatny poziom cyberbezpieczeństwa ochrony prywatności pacjenta w zakresie rodzaju wdrożonych usług i rodzaju przetwarzanych danych, w szczególności. Jeżeli projekt nie dotyczy danego obszaru wpisz ND. | |
| 1. systemy teleinformatyczne świadczeniodawcy zapewnią dwuskładnikowe uwierzytelnienie wszystkich użytkowników |  |
| 2.systemy teleinformatyczne świadczeniodawcy będą posiadały firewall, pozwalający analizować przesyłane pakiety pod względem ich treści wraz z wdrożeniem w infrastrukturze teleinformatycznej przez osobę posiadającą kompetencje z zakresu bezpieczeństwa sieci. Efektem wdrożenia musi być wykonanie zewnętrznych skanów podatności, które wykażą brak podatności krytycznych oraz podatności, które mogą doprowadzić do incydentu poważnego w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Wnioskodawca jest zobowiązany do utwardzania konfiguracji do momentu uzyskania wskazanego efektu. Wyeliminowanie podatności będzie potwierdzone przez audyt bezpieczeństwa |  |
| 3.podmiot wykonujący działalność leczniczą będzie miał wdrożony i utrzymywany system zarządzania bezpieczeństwem informacji, opracowany i wdrożony na podstawie Polskiej Normy PN-ISO/IEC 27001, i ciągłością działania. Nadzór nad systemem będzie sprawowany przez osobę, której zakres obowiązków nie budzi konfliktu interesów (np. nadzoru nie może sprawować komórka organizacyjna odpowiedzialna za IT) |  |
| 4.system kopii zapasowych będzie umożliwiać realizację kopii zapasowej za pomocą streamera lub biblioteki taśmowej. Kopie te będą przechowywane w innej lokalizacji niż środowisko produkcyjne, np. inny budynek, a w przypadku braku takiej możliwości, w pomieszczeniu oddalonym od serwerowni. System ten będzie umożliwiać odtworzenie kopii zapasowej i testowe odtworzenie systemów w środowisku testowym. Cały proces będzie opisany procedurą stanowiącą element dokumentacji bezpieczeństwa. Możliwe będzie również wdrożenie innego systemu wykonywania kopii zapasowych, który nie będzie oparty na taśmach magnetycznych, jednak musi on być skonfigurowany przez osobę posiadającą kompetencje z zakresu realizacji systemów kopii zapasowych, gwarantującą wykonanie skutecznych kopii zapasowych oraz konfigurację separacji sieciowej. Utworzenie odmiejscowej kopii zapasowej i odtworzenie z niej kompletnego systemu oraz wykonanej  dokumentacji zostanie potwierdzone poprzez wynik przeprowadzonego audytu systemu kopii zapasowej |  |
| 5.system poczty elektronicznej wraz z systemem bezpieczeństwa, będzie obejmował mechanizmy SPF (Sender Policy Framework), DMARC (Domain- based Message Authentication Reporting and Conformance), DKIM (DomainKeys Identified Mail), antyspam oraz ochronę antywirusową, a skuteczność wdrożenia ww. mechanizmów zostanie potwierdzona przeprowadzonym audytem systemu poczty elektronicznej |  |
| 6.na stacjach roboczych i serwerach świadczeniodawcy zostanie zainstalowany system oparty na rozwiązaniach co najmniej klasy Endpoint Detection and Response w architekturze klient – serwer na wszystkich stacjach roboczych oraz serwerach świadczeniodawcy wraz z jego wdrożeniem w infrastrukturze teleinformatycznej przez osobę posiadającą kompetencje z zakresu realizacji systemów antywirusowych. Prawidłowość wdrożenia systemu potwierdzi przeprowadzony audyt systemu na wszystkich stacjach roboczych oraz serwerach świadczeniodawcy |  |
| 7.zostaną przeprowadzone skany podatności oraz testy penetracyjne wewnętrznych systemów usługodawców, w wyniku których nastąpi konfiguracja, mająca na celu usunięcie wykrytych podatności (utwardzenie systemów) |  |
| 8.systemy teleinformatyczne usługodawcy zapewnią zgodność z art. 32 Rozporządzenia Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE |  |
| 9.zapewniona zostanie zgodność z narodowymi standardami bezpieczeństwa:  a) NSC 200, Minimalne wymagania bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych,  b)NSC 800-53, Zabezpieczenia i ochrona prywatności systemów informacyjnych oraz organizacji |  |
| 10.ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie będzie odbywało się na podstawie Polskich Norm:  a) PN-ISO/IEC 27002 - w odniesieniu do ustanawiania zabezpieczeń,  b) PN-ISO/IEC 27005 - w odniesieniu do zarządzania ryzykiem? |  |

*………….……………………………..*

*Podpis osoby upoważnionej*

*do reprezentowania wnioskodawcy*