Uchwała Nr 27/2023/IV
Komitetu Sterującego do spraw koordynacji wsparcia w sektorze zdrowia
z dnia 11 grudnia 2023 r.
w sprawie przyjęcia rekomendacji dla kryteriów wyboru projektów
w obszarze e-zdrowia oraz telemedycyny realizowanych w ramach programów regionalnych
w zakresie celu szczegółowego 1 (ii) *Czerpanie korzyści z cyfryzacji dla obywateli, przedsiębiorstw, organizacji badawczych i instytucji publicznych*

Na podstawie § 5 ust. 1 Regulaminu Komitetu Sterującego do spraw koordynacji wsparcia w sektorze zdrowia, Komitet Sterujący do spraw koordynacji wsparcia w sektorze zdrowia uchwala, co następuje:

§ 1.

Przyjmuje się „Rekomendacje dla kryteriów wyboru projektów w obszarze e-zdrowia oraz telemedycyny realizowanych w ramach programów regionalnych w zakresie celu szczegółowego 1 (ii) *Czerpanie korzyści z cyfryzacji dla obywateli, przedsiębiorstw, organizacji badawczych i instytucji publicznych*", stanowiące załącznik do niniejszej uchwały.

§ 2.

Uchwała wchodzi w życie z dniem podjęcia.

Małgorzata Majewska
/dokument podpisany elektronicznie/
Przewodniczący
Komitetu Sterującego do spraw koordynacji
wsparcia w sektorze zdrowia

Załącznik do Uchwały 27/2023/IV z dnia 11 grudnia 2023 r.

Rekomendacje dla kryteriów wyboru projektów w obszarze e-zdrowia oraz telemedycyny realizowanych w ramach programów regionalnych w zakresie celu szczegółowego 1 (ii)
***Czerpanie korzyści z cyfryzacji dla obywateli, przedsiębiorstw, organizacji badawczych i instytucji publicznych*[1]**

I. Zasady ogólne – specyficzne dla obszaru e-zdrowia i telemedycyny[2]

1. Rekomendacje dla kryteriów wyboru projektów mają zastosowanie do projektów z obszaru e-zdrowia i telemedycyny wybieranych w sposób niekonkurencyjny oraz sposób konkurencyjny.
2. W przypadku naborów realizowanych w trybie konkurencyjnym oraz i projektów wybieranych w sposób niekonkurencyjny wykraczających poza ww. obszar, np. dotyczących wszystkich e-usług publicznych (w których nie jest możliwe przyjęcie kryteriów wyboru projektów w obszarze e-zdrowia i/lub telemedycyny), Instytucje Zarządzające powinny w inny sposób zapewnić, że wybierane do dofinansowania projekty w części dotyczącej e-zdrowia i/lub telemedycyny są zgodne z poniższymi Rekomendacjami[3].
3. Warunkiem rozpoczęcia realizacji wsparcia w obszarze e-zdrowia i telemedycyny jest uzyskanie pozytywnej opinii MZ w zakresie zgodności projektów wybieranych w sposób konkurencyjny/projektu wybieranego w sposób niekonkurencyjny z dokumentami strategicznymi i programowymi w obszarze zdrowia cyfrowego oraz jego komplementarności i interoperacyjności z rozwiązaniami w zakresie e-zdrowia i telemedycyny, obowiązującymi na dzień złożenia wniosku o wydanie opinii na zasadach określonych w § 9 ust. 6 pkt 1 *Regulaminu Komitetu Sterującego do spraw koordynacji wsparcia w sektorze zdrowia*.[4]
4. Do dofinansowania mogą być przyjęte wyłącznie projekty zgodne z „Programem rozwoju e-zdrowia na lata 2022-2027”[5]. Przy czym projekty oceniane i przyjmowane są do dofinansowania na podstawie wersji „Programu rozwoju e-zdrowia na lata 2022 – 2027” obowiązującej na dzień złożenia wniosku o wydanie opinii na zasadach określonych w § 9 ust. 6 pkt 1 Regulaminu Komitetu Sterującego do spraw koordynacji wsparcia w sektorze zdrowia.
5. Kryteria są zgodne z aktualnymi na dzień ich zatwierdzania rekomendacjami Komitetu Rady Ministrów do Spraw Cyfryzacji (KRMC), w szczególności zawartymi w Portalu Interoperacyjności i Architektury, w tym dla kryteriów wyboru projektów z zakresu

---

[1] Dla pozostałych celów szczegółowych rekomendacje mają zastosowanie w przypadku, gdy wartość komponentu e-zdrowia lub telemedycyny stanowi ponad 20% wartości projektu oraz wynosi minimum 2 mln zł.

[2] Zasady ogólne określone w niniejszym załączniku do *Uchwały* stanowią dodatkowe zasady w stosunku do zasad ogólnych zawartych w załączniku do *Uchwały Nr 5/2023/II Komitetu Sterującego do spraw koordynacji wsparcia w sektorze zdrowia z dnia 28 sierpnia 2023 r. w sprawie przyjęcia zasad ogólnych dla projektów realizowanych w obszarze zdrowia* . Do projektów w obszarze e-zdrowia oraz telemedycyny w ramach programów regionalnych zastosowanie mają zasady określone w obu Uchwałach.

[3] Np. poprzez właściwe zapisy SZOP lub określenie minimalnych warunków dotyczących działań w projektach w zakresie e-zdrowia i/lub telemedycyny w regulaminie wyboru projektów.

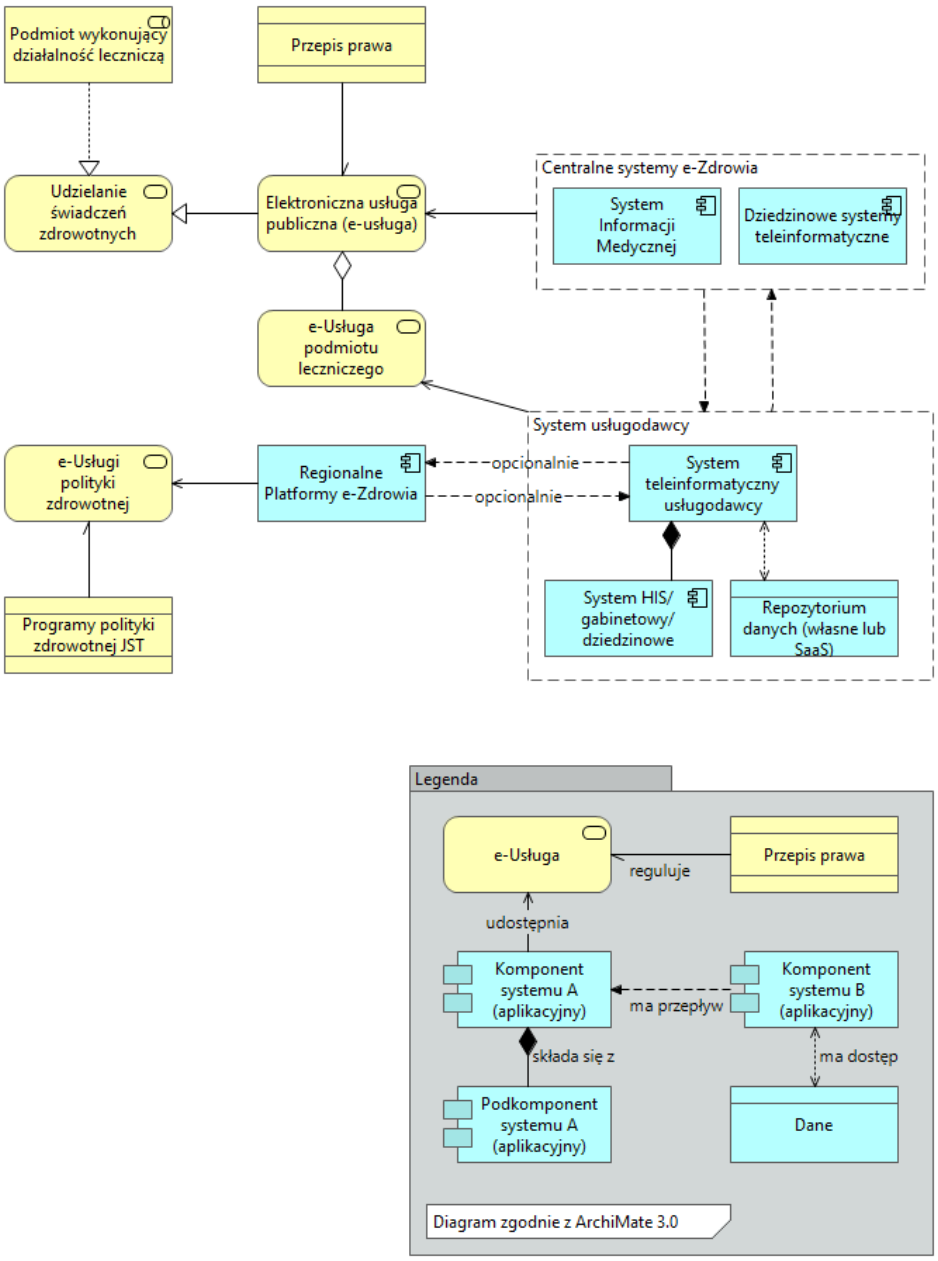
[4] Regulamin przyjęty Uchwałą Nr 1/2023/I Komitetu Sterującego do spraw koordynacji wsparcia w sektorze zdrowia z dnia 27 czerwca 2023 r. w sprawie przyjęcia regulaminu Komitetu Sterującego do spraw koordynacji wsparcia w sektorze zdrowia.

[5] Program zamieszczony został na stronie internetowej: https://www.gov.pl/web/zdrowie/program-rozwoju-e-zdrowia-na-lata-2022-2027.

usług elektronicznych, z uwzględnieniem ewentualnych zmian ww. rekomendacji[6]. Kryteria muszą być zgodne w szczególności z Pryncypiami Architektury Informacyjnej Państwa, modelem realizacji e-usługi oraz zasadami budowy interoperacyjnego systemu teleinformatycznego.

6. Kryteria muszą zapewniać realizację wymagań w zakresie integracji systemów usługodawców z centralnymi systemami e-zdrowia oraz wymagań w zakresie budowy lub rozbudowy przez świadczeniodawców elektronicznych usług publicznych (e-usług), określonych w przepisach obowiązującego prawa oraz wytycznych/rekomendacjach właściwych instytucji, w tym wymagań w zakresie cyberbezpieczeństwa i ochrony danych osobowych. Architektura wdrażanych e-usług powinna być zgodna z poniższym rysunkiem. e-Usługi podmiotu leczniczego powinny być elementem e-usług świadczonych przez systemy centralne i powinny być świadczone poprzez integrację systemu usługodawcy z centralnymi systemami e-zdrowia. Zgodnie z Programem rozwoju e-zdrowia e-usługi będą budowane na poziomie centralnym, usługodawcy powinni dostosować się do projektowanych e-usług i świadczyć je poprzez integrację z centralnymi systemami e-zdrowia. Jednostki samorządu terytorialnego powinny tworzyć i rozwijać e-usługi związane z potrzebami społeczeństwa w perspektywie regionalnej i lokalnej wyłącznie wspierające realizację samorządowych programów polityki zdrowotnej, w tym np. związane z profilaktyką chorób. Istniejące lub powstające e-usługi winny być utrzymywane przy zachowaniu interoperacyjności oraz komplementarności z usługami na poziomie krajowym, z uwzględnieniem potrzeb określonych w samorządowych programach polityki zdrowotnej.

[6] Portal Interoperacyjności i Architektury: https://www.gov.pl/web/ia



Rysunek 1 Metamodel realizacji e-usługi

II. Rekomendacje dla kryteriów dostępu

1. Kryteria zapewniają komplementarność i interoperacyjność inwestycji zaplanowanych we wnioskach o dofinasowanie projektów z innymi już zrealizowanymi i realizowanymi projektami z obszaru e-zdrowia oraz zgodność z dokumentami strategicznymi i programowymi w obszarze zdrowia cyfrowego[7] publikowanymi na BIP MZ oraz na stronie www.ezdrowie.gov.pl.
2. Kryteria zapewniają zgodność produktów wytworzonych w projekcie ze standardami wymiany oraz formatami elektronicznej dokumentacji medycznej (dalej: EDM) oraz standardami komunikacji, o których mowa w art. 8d *ustawy z dnia 28 kwietnia 2011 r.*

[7] Oznacza to, że projekty, w tym m.in. polegające na dostosowaniu systemów teleinformatycznych usługodawców do wymiany danych z Systemem Informacji Medycznej lub z systemami innych usługodawców, będą weryfikowane pod kątem komplementarności, interoperacyjności oraz niedublowania funkcjonalności przewidzianych w usługach centralnych (np. Systemu Informacji Medycznej (P1 i P2), systemami dziedzinowymi, systemem e-Krew).

o systemie informacji w ochronie zdrowia (Dz.U. z 2022 r. poz. 1555, z późn. zm., dalej: USIOZ), które zostaną zamieszczone w Biuletynie Informacji Publicznej urzędu obsługującego ministra właściwego do spraw zdrowia na zasadach określonych w art. 8d ust. 2–6 USIOZ.

3. **Kryteria zapewniają, że projekt dotyczący:**

   - budowy i rozbudowy e-usług - jeśli zasadne - za pośrednictwem rozwiązań centralnych, w szczególności obejmujący prowadzenie lub wymianę EDM albo rozwiązań telemedycznych,
   - budowy/rozbudowy narzędzi teleinformatycznych (dotyczy działań prowadzanych przez podmioty wykonujące działalność leczniczą) w celu usprawnienia procesu udzielania świadczeń (back-office) oraz świadczenia e-usług (w szczególności taką usługą jest wymiana EDM),

   zapewni rozwiązania (w obszarach, których dotyczy projekt):

   3.1. W obszarze gromadzenia i wymiany danych medycznych:

   3.1.1. Zlecenia procedur medycznych (badań, konsultacji, podania leków) oraz przekazanie wyników tych procedur personelowi medycznemu - po zakończeniu realizacji projektu będą w całości realizowane w systemach teleinformatycznych (np. w systemie szpitalnym HIS, gabinetowym, laboratoryjnym LIS, radiologicznym RIS, farmaceutycznym PIS, kardiologicznym CIS);

   3.1.2. Ponad 90% obrazów medycznych (DICOM, nie-DICOM) oraz wyników badań laboratoryjnych wytworzone po zakończeniu realizacji projektu będzie przechowywanych w systemie teleinformatycznym, a dane te będą powiązane z danymi pacjenta oraz zdarzeniami medycznymi w ramach których były realizowane;

   3.1.3. Ponad 90% wyników badań laboratoryjnych wytworzonych po zakończeniu realizacji projektu (m.in. biochemia kliniczna, mikrobiologia, badania molekularne) będzie przechowywanych w formie ustrukturyzowanych danych, które można wykorzystać w ramach analiz niezbędnych do podejmowania decyzji klinicznych;

   3.1.4. W procesie zarządzania podawaniem leków po zakończeniu realizacji projektu będą wykorzystywane interaktywne alerty, zapewniające bezpieczeństwo podawania leków (np. zduplikowane zlecenia, interakcje leków, nieprawidłowe dawki itd.). Podmioty wykonujące działalność leczniczą będą gromadzić dane o wszystkich produktach leczniczych podanych pacjentowi w trakcie udzielania świadczeń wraz z dawką i czasem podania;

   3.1.5. Po zakończeniu realizacji projektu podmiot wykonujący działalność leczniczą posiada system informatyczny zgodny z wymaganiami art. 8b USIOZ. W ramach tego kryterium należy m.in. weryfikować 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;

3.1.6. Po zakończeniu realizacji projektu w systemie teleinformatycznym usługodawcy powinien umożliwiać (upoważnionym pracownikom medycznym) pobranie EDM pacjenta wytworzonej w innych podmiotach wykonujących działalność leczniczą.

3.2. W obszarze analityki medycznej:

3.2.1. W wyniku realizacji projektu zostały określone zasady oraz procedury dotyczące przepływu danych medycznych w podmiocie, w tym m.in. zasady skanowania danych przy łóżku pacjenta (skanowania z wykorzystaniem czytników kodów kreskowych/QR);

3.2.2. Komórki organizacyjne, jednostki, podmioty będą raportować wyniki dotyczące efektywności finansowej oraz działalności podstawowej (medycznej) - efektywności i jakości procesu leczenia. Podmiot wykonujący działalność leczniczą będzie agregował te dane w celu wykorzystania do zarządzania jakością i efektywnością. Raporty będą przeznaczone dla personelu medycznego monitującego skuteczność leczenia pacjentów, kadry zarządzającej podmiotem leczniczym oraz dla podmiotów tworzących, nadzorujących działanie podmiotów podległych.

3.3. W obszarze cyberbezpieczeństwa zostanie zapewniony adekwatny poziom cyberbezpieczeństwa ochrony prywatności pacjenta w zakresie rodzaju wdrożonych usług i rodzaju przetwarzanych danych, w szczególności:

3.3.1. Systemy teleinformatyczne świadczeniodawcy zapewnią dwuskładnikowe uwierzytelnienie wszystkich użytkowników;

3.3.2. Firewall pozwalający analizować przesyłane pakiety pod względem ich treści wraz z wdrożeniem w infrastrukturze teleinformatycznej świadczeniodawcy przez osobę posiadającą kompetencje z zakresu bezpieczeństwa sieci.

Efektem wdrożenia musi być wykonanie zewnętrznych skanów podatności, które wykażą brak podatności krytycznych oraz które mogą doprowadzić do incydentu poważnego w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2022 r. poz. 1863, z późn. zm.). Wnioskodawca jest zobowiązany do utwardzania konfiguracji do momentu uzyskania wskazanego efektu. Wyeliminowanie podatności musi być potwierdzone przez audyt bezpieczeństwa;

3.3.3. 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 jest sprawowany przez osobę, której zakres obowiązków nie budzi konfliktu interesów (np. nadzoru nie może sprawować komórka organizacyjna odpowiedzialna za IT);

3.3.4. System kopii bezpieczeństwa;

System kopii zapasowych musi umożliwiać realizację kopii zapasowej za pomocą streamera lub biblioteki taśmowej. Kopie te muszą być przechowywane w innej lokalizacji niż środowisko produkcyjne, np. inny budynek, a w przypadku braku takiej możliwości, w pomieszczeniu oddalonym od serwerowni. System ten powinien umożliwiać odtworzenie kopii zapasowej i testowe odtworzenie systemów w środowisku testowym. Cały proces musi być opisany procedurą stanowiącą element dokumentacji bezpieczeństwa. Możliwe jest 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.

Efektem realizacji musi być przeprowadzenie audytu systemu kopii zapasowej, którego wynik potwierdzi utworzenie odmiejscowionej kopii zapasowej i odtworzenie z niej kompletnego systemu oraz wykonanej dokumentacji bezpieczeństwa;

3.3.5. Zapewnienie bezpieczeństwa poczty elektronicznej;

System poczty elektronicznej wraz z systemem bezpieczeństwa, który będzie obejmował mechanizmy SPF, DMARC, DKIM, antyspam oraz ochronę antywirusową.

Efektem realizacji musi być przeprowadzenie audytu systemu poczty elektronicznej, którego wynik potwierdzi skuteczność wdrożenia SPF, DMARC, DKIM, antyspam oraz ochronę antywirusową.

SPF: Sender Policy Framework - niekomercyjny projekt mający na celu wprowadzenie zabezpieczenia serwerów SMTP przed przyjmowaniem poczty z niedozwolonych źródeł. Ma to pozytywnie wpłynąć na ograniczenie liczby wiadomości mailowych będących spamem,

DMARC: (Domain-based Message Authentication Reporting and Conformance) - możliwość ochrony domeny przed nieautoryzowanym użyciem, powszechnie znanym jako fałszowanie wiadomości e-mail,

DKIM: (DomainKeys Identified Mail) - metoda łączenia domeny internetowej z wiadomością e-mail, która pozwala organizacji brać odpowiedzialność za treść e-maila. Sygnatura DKIM zabezpiecza przed podszywaniem się pod nadawcę z innych domen

3.3.6. Został zainstalowany system Endpoint Detection and Response na stacjach roboczych i serwerach;

Systemy oparte na rozwiązaniach co najmniej klasy Endpoint Detection and Response w architekturze klient - serwer na wszystkich stacjach roboczych oraz serwerach świadczeniodawcy wraz z wdrożeniem w infrastrukturze teleinformatycznej świadczeniodawcy przez osobę posiadającą kompetencje z zakresu realizacji systemów antywirusowych.

Efektem realizacji musi być przeprowadzenie audytu systemu Endpoint Detection and Response, na wszystkich stacjach roboczych oraz serwerach świadczeniodawcy, który potwierdzi prawidłowość wdrożenia systemu.

3.3.7. Zostaną przeprowadzone skany podatności oraz testy penetracyjne wewnętrznych systemów usługodawców. W wyniku powyższych działań zostaną przeprowadzone konfiguracje, mające na celu usunięcie wykrytych podatności (utwardzenie systemów);

3.3.8. 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 (ogólne rozporządzenie o ochronie danych).

3.3.9. Zapewniono zgodność z narodowymi standardami cyberbezpieczeństwa[8]:
a) NSC 200, Minimalne wymagania bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych,
b) NSC 800-53, Zabezpieczenia i ochrona prywatności systemów informacyjnych oraz organizacji;

3.3.10. Ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie będzie odbywało się na podstawie Polskich Norm związanych z tą normą, w tym:
a) PN-ISO/IEC 27002 - w odniesieniu do ustanawiania zabezpieczeń;
b) PN-ISO/IEC 27005 - w odniesieniu do zarządzania ryzykiem;

4. **Kryteria zapewniają, że projekt w zakresie budowy lub rozbudowy regionalnej platformy e-zdrowia (jeżeli platforma taka jest planowana) uwzględnia:**

4.1. Usługi dotyczące repozytorium EDM w modelu oprogramowania jako usługa (SaaS) świadczone dla podmiotów leczniczych z regionu. Repozytorium EDM powinno realizować co najmniej usługę przyjmowania, archiwizacji i udostępniania EDM zgodnej z HL7 CDA oraz standardami udostępniania danych medycznych zamieszczonymi w Biuletynie Informacji Publicznej ministra właściwego do spraw zdrowia, w tym co najmniej ze standardem DICOM - w przypadku gdy repozytorium EDM obejmuje dane obrazowe;

4.2. Usługi wspierające realizację samorządowych programów polityki zdrowotnej, w szczególności związane z profilaktyką chorób;

4.3. Wspólną infrastrukturę techniczno-systemową, co najmniej w zakresie zapasowych ośrodków przetwarzania danych, oferowaną podmiotom wykonującym działalność leczniczą z danego regionu;

4.4. Budowę centrum monitorowania zagrożeń cyberbezpieczeństwa (SOC) z możliwością monitorowania infrastruktury podmiotów wykonujących działalność leczniczą z danego regionu;

5. **Kryteria zapewniają, że projekt w zakresie budowy lub rozbudowy regionalnej platformy e-zdrowia (jeżeli platforma taka jest planowana)** spełnia standardy dostępności cyfrowej WCAG 2.1. na poziomie AA oraz zgodność z przepisami krajowymi i europejskimi w tym zakresie, w tym z dyrektywą (UE) 2016/2102 w sprawie dostępności stron internetowych i mobilnych aplikacji organów sektora publicznego.

[8] Narodowe Standardy Cyberbezpieczeństwa (NSC), to zbiór rekomendacji standaryzujących rozwiązania zabezpieczające w sieciach i systemach informacyjnych wykorzystywanych przez podmioty chcące efektywnie zarządzać systemami bezpieczeństwa informacji. Zawierają one wytyczne w zakresie budowanie efektywnego systemu zarządzania bezpieczeństwem informacji w oparciu o praktykę stosowaną w administracji federalnej USA. Są one wydawane przez Pełnomocnika Rządu do spraw Cyberbezpieczeństwa, w ramach celu szczegółowego 2 Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024.

III. Rekomendacje dla kryteriów premiujących

1. Kryteria premiują objęcie jak najszerszego kręgu podmiotów wykonujących działalność leczniczą w danym województwie bez względu na podmiot tworzący.
2. Kryteria premiują projekty, które w zakresie budowy lub rozbudowy e-usług lub narzędzi teleinformatycznych wykorzystywanych w podmiocie wykonującym działalność leczniczą będą oparte na potrzebach pacjentów i kadry medycznej.

   Potwierdzeniem spełnienia tego kryterium powinny być zapisy dokumentacji projektowej potwierdzające udział pacjentów i kadry medycznej np. w definiowaniu wymagań, zatwierdzaniu zmian w procesach biznesowych oraz potwierdzający aktywny udział w testach.
3. Kryteria powinny uwzględniać aktywny udział kadry zarządczej (odpowiedzialnych za przebieg procesów biznesowych w podmiotach) w planowaniu, rozbudowie i produkcyjnym wdrażaniu usług i funkcjonalności ujętych w projekcie. Jest to działanie niezbędne do zwiększenia dojrzałości cyfrowej podmiotów wykonujących działalność leczniczą.

   Potwierdzeniem spełnienia tego kryterium powinny być zapisy dokumentacji projektowej potwierdzające udział kadry zarządzającej np. w definiowaniu wymagań, zatwierdzaniu zmian w procesach biznesowych oraz potwierdzający aktywny udział w testach.
4. **Kryteria w zakresie projektów dotyczących:**
   - budowy i rozbudowy e-usług, w szczególności obejmujących prowadzenie lub wymianę EDM albo rozwiązań telemedycznych,
   - budowy/rozbudowy narzędzi informatycznych w celu usprawnienia procesu udzielania świadczeń (back-office) oraz świadczenia e-usług (w szczególności taką usługą jest wymiana EDM),

   premiują następujące rozwiązania (w obszarach, których dotyczy projekt):

   4.1 Rozwiązania pozwalające na przetwarzanie danych medycznych:

   4.1.1 Wyniki badań laboratoryjnych i diagnostycznych (w tym obrazowych) będą gromadzone w jednym repozytorium (repozytorium może być skompilowane przy użyciu jednego programu lub wielu modułów oprogramowania działających jako jedno repozytorium), a personel medyczny udzielający świadczeń ma dostęp do tych wyników zgodnie z zakresem kompetencji;

   4.1.2 Personel medyczny ma dostęp (także przy łóżku pacjenta) do kart/danych/raportów pacjenta. Podczas każdego świadczenia następuje weryfikacja czy w innych podmiotach leczniczych nie zostały wytworzone dla Pacjenta dokumenty stanowiące EDM. Wszystkie wyniki procedur medycznych (badań, konsultacji, podania leków) są dostępne dla pracowników medycznych udzielających świadczeń zdrowotnych. Wszystkie wyniki procedur medycznych (badań, konsultacji, podania leków) będą powiązane z jednym rekordem zdrowotnym Pacjenta oraz zdarzeniami medycznymi, w ramach których były realizowane.

   4.1.3 W ramach cyfrowych zleceń zostaną zaimplementowane podstawowe funkcje wspomagania decyzji (np. weryfikacja zduplikowania zlecenia, interakcje leków itp.);

4.1.4 We wszystkich lokalizacjach zainstalowana zostanie infrastruktura pozwalająca na wykorzystywanie skanowania (np. w zakresie leków, próbek krwi itd.) przy łóżku pacjenta;

4.1.5 W obszarach biznesowych, w których wykorzystanie telemedycyny jest możliwe, uzasadnione i generuje wartość dodaną dla komfortu i bezpieczeństwa pacjenta, działania powinny być ukierunkowane na wykorzystanie rozwiązań telemedycznych.

Telemedycyna może zostać wykorzystana do bezpośredniego udzielania świadczeń, wsparcia pracowników medycznych w udzielaniu świadczeń (np. telekonsultacje pracownik - pracownik) lub monitorowania pacjentów;

4.2 Rozwiązania przynoszące korzyści dla pacjenta:

4.2.1 Pacjenci w trakcie procesu leczenia mają dostęp do danych medycznych w czasie rzeczywistym, co pozwala im oceniać postępy w zakresie celów związanych ze zdrowiem, oraz szczegółowej dokumentacji ścieżki/planu opieki i produktów stosowanych w jej ramach (np. implantów, leków) – kryterium dotyczy podmiotów wykonujących działalność leczniczą udzielających świadczeń w rodzaju leczenie szpitalne;

4.2.2 Zgłaszanie zdarzeń niepożądanych jest zautomatyzowane (np. identyfikowanie numerów partii i serii poszczególnych produktów w celu identyfikowania sprzedawcy w skali globalnej);

4.2.3 Pacjenci otrzymują alerty, przypomnienia i powiadomienia związane ze ścieżkami/planami opieki, które mają pomóc w samodzielnej realizacji zaleceń oraz wytycznych w procesie leczniczym.

4.3 W obszarze analityki medycznej:

Podmioty określiły wyniki docelowe w działalności ekonomiczno-finansowej i działalności podstawowej (medycznej) i każdego roku raportują dane w odniesieniu do tych wyników.

4.4 W obszarze cyberbezpieczeństwa (zapewniającym adekwatny poziom cyberbezpieczeństwa ochrony prywatności pacjenta w zakresie rodzaju wdrożonych usług i rodzaju przetwarzanych danych):

Zostanie przeprowadzony audyt bezpieczeństwa zgodnie z wytycznymi CeZ;

5. Kryteria premiują projekty zawierające rozwiązania synergiczne - typu grupowe zakupy systemów wsparcia (oprogramowanie, sprzęt, usługi itp.) czy tworzenie centrów kompetencji, które zapewnią wsparcie m.in. w zakresie budowy architektury systemów informacyjnych, zakupu usług, ITS i oprogramowania oraz przygotowania OPZ.
6. Kryteria premiują, w odniesieniu do projektów z zakresu telemedycyny, działania ukierunkowane na deinstytucjonalizację opieki zdrowotnej poprzez rozwój opieki nad pacjentem w warunkach domowych (np. telemonitoring).
7. Kryteria premiują projekty, w ramach których realizowane są szkolenia dotyczące przedmiotu projektu, w tym cyberbezpieczeństwa dla personelu podmiotów wykonujących działalność leczniczą udzielających świadczeń opieki zdrowotnej dotyczących przedmiotu projektu.