ZARZĄDZENIE NR 68/2022/BBIICD
PREZESA NARODOWEGO FUNDUSZU ZDROWIA

z dnia 20 maja 2022 r.

w sprawie finansowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców

Na podstawie art. 102 ust. 5 pkt 21 i 25 ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. z 2021 r. poz. 1285, z późn. zm.[1)]) oraz polecenia Ministra Zdrowia z dnia 29 kwietnia 2022 r., znak: DIWP.07.5.2022.KW, wydanego na podstawie 11h ust. 2 pkt 2 i ust. 4 ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID- 19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz. U. z 2021 r. poz. 2095, z późn. zm.[2)]), zarządza się, co następuje:

Rozdział 1.
Postanowienia ogólne

§ 1. Zarządzenie określa warunki przyznawania i rozliczania środków na finansowanie działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych u świadczeniodawców.

2. Finansowanie, o którym mowa w ust. 1, przyznawane jest świadczeniodawcom, będącym podmiotami leczniczymi, o których mowa w art. 4 ust. 1 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz. U. z 2022 r. poz. 633, 655 i 974) prowadzącymi szpital i posiadającymi umowę o udzielanie świadczeń opieki zdrowotnej zawartą z Narodowym Funduszem Zdrowia obowiązującą w 2021 r. oraz 2022 r., w rodzaju:

1) leczenie szpitalne lub

2) rehabilitacja lecznicza, lub

3) opieka psychiatryczna i leczenie uzależnień, lub

4) lecznictwo uzdrowiskowe.

3. Finansowanie, o którym mowa w ust. 1, obejmuje wydatki świadczeniodawców ponoszone od dnia 29 kwietnia 2022 r. do dnia 31 grudnia 2022 r.

§ 2. Użyte w zarządzeniu określenia oznaczają:

1) dyrektor właściwego oddziału Funduszu - dyrektora oddziału wojewódzkiego Narodowego Funduszu Zdrowia, właściwy w zakresie realizacji umowy o udzielanie świadczeń opieki zdrowotnej, o której mowa w § 1 ust. 2;

2) Fundusz – Narodowy Fundusz Zdrowia;

3) oddział Funduszu - oddział wojewódzki Funduszu.

Rozdział 2.
Warunki udzielania finansowania

§ 3. 1. Finansowaniem, o którym mowa w § 1, w okresie do dnia 31 grudnia 2022 r., są objęte działania podnoszące poziom bezpieczeństwa systemów teleinformatycznych świadczeniodawców, z zastrzeżeniem ust. 2, i polegające na wykonaniu co najmniej jednej z następujących czynności:

1) zakup i wdrożenie systemów teleinformatycznych, w tym urządzeń, oprogramowania i usług zapewniających prewencję, reakcję i detekcję zagrożeń cyberbezpieczeństwa, w szczególności:

   a) systemów kopii bezpieczeństwa, odmiejscowienia kopii, segmentacji w celu odseparowania urządzeń backupu, zapewnienia mechanizmów weryfikacji poprawności i odtwarzalności kopii i backupu,

---

[1)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2021 r. poz. 1292, 1559, 1773, 1834, 1981, 2120, 2232 i 2270 oraz z 2022 r. poz. 64, 91, 526, 583, 655, 807, 974 i 1002.

[2)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2021 r. poz. 2120, 2133, 2262, 2269, 2317, 2368 i 2459 oraz z 2022 r. poz. 202, 218, 655 i 830

b) systemów antywirusowych dla stacji roboczych i serwerów - centralnie zarządzanych, systemów klasy Endpoint Detection and Response (EDR),

c) systemów kontroli dostępu administracyjnego, zarządzania uprawnieniami (IAM/IDM),

d) urządzeń i oprogramowania typu firewall - zapora sieciowa z wbudowanym IPS oraz systemem antywirusowym oraz platform niezbędnych do ich uruchomienia,

e) systemów zapewniających bezpieczny system poczty elektronicznej, włączając w to systemy weryfikacji załączników i treści korespondencji oraz systemy wieloskładnikowego uwierzytelniania,

f) rozwiązań zapewniających ochronę DNS (DNS Protection) z użyciem systemów lokalnych (licencja oraz wsparcie w okresie do dnia 31 grudnia 2022 r.),

g) systemu typu SIEM,

h) systemu typu NAC – jako system lokalny;

2) zakup usługi wdrożenia i konfiguracji urządzeń i oprogramowania, o których mowa w pkt 1, oraz wsparcia eksperckiego w zakresie cyberbezpieczeństwa przez okres do dnia 31 grudnia 2022 r.;

3) zakup i wdrożenie systemu (usługi) typu SOC – przez okres do dnia 31 grudnia 2022 r.;

4) zakup usługi skanów podatności, w zakresie sprecyzowanym w materiale referencyjnym „Plan działania w zakresie cyberbezpieczeństwa w ochronie zdrowia", opublikowanym na stronie internetowej Centrum e-Zdrowia[3)], przez okres do dnia 31 grudnia 2022 r.;

5) zakup opracowania wraz z przekazaniem praw autorskich dokumentacji systemu zarządzania bezpieczeństwem informacji zgodnie z wymaganiami ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2021 r. poz. 2070), rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247), oraz ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369, z 2021 r. poz. 2333 i 2445 oraz z 2022 r. poz. 655) - jeśli dotyczy świadczeniodawcy będącego operatorem usługi kluczowej, o którym mowa w art. 5 tej ustawy, w tym planu odtworzenia po awarii;

6) zakup szkolenia lub szkoleń w zakresie cyberbezpieczeństwa skierowanych do kadry zarządzającej świadczeniodawcą oraz osób zatrudnionych u świadczeniodawcy w zakresie podstawowej świadomości bezpieczeństwa IT, w tym:

a) ochrony przed zaawansowanymi atakami przez pocztę i WWW,

b) tworzenia i zarządzania polityką haseł i tożsamości,

c) zarządzania ryzykiem, dokumentacją i polityką bezpieczeństwa w jednostkach publicznych w świetle rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247),

d) wykonywania kopii zapasowych oraz tworzenia i utrzymania polityki ciągłości działania.

2. Czynności, o których mowa w ust. 1, mogą zostać objęte finansowaniem wyłącznie w przypadku wykazania przez świadczeniodawcę, wynikiem audytu bezpieczeństwa, zwiększenia poziomu bezpieczeństwa systemów teleinformatycznych wykorzystywanych do udzielania świadczeń opieki zdrowotnej.

3. Fundusz dokona weryfikacji zmian poziomu bezpieczeństwa teleinformatycznego świadczeniodawcy na podstawie wypełnionej i złożonej przez niego, przed przystąpieniem do czynności, o których mowa w ust. 1, wynikających z niniejszego zarządzenia, ankiety badającej poziom bezpieczeństwa systemów teleinformatycznych tego świadczeniodawcy, o której mowa w ust. 5, oraz wyniku audytu bezpieczeństwa potwierdzającego zwiększenie poziomu bezpieczeństwa teleinformatycznego u świadczeniodawcy. Ankieta powinna być złożona wraz z wnioskiem o zawarcie umowy zgodnie z ust. 8.

[3)] https://cez.gov.pl/pl/page/o-nas/aktualnosci/plan-dzialania-w-zakresie-cyberbezpieczenstwa-w-ochronie-zdrowia

4. Finansowanie mogą otrzymać świadczeniodawcy spełniający określone w niniejszym zarządzeniu warunki, zgodnie z kolejnością składania spełniających wymogi formalne wniosków, do wyczerpania środków publicznych, o których mowa w ust. 6, którzy złożą oświadczenia o braku finansowania tych samych czynności (w tym zakupów urządzeń, oprogramowania, licencji, usług IT) z jakichkolwiek innych środków publicznych zewnętrznych, w tym krajowych bądź europejskich (wykluczenie podwójnego finansowania).

5. Warunkiem ubiegania się przez świadczeniodawcę o finansowanie jest przeprowadzenie badania poziomu dojrzałości cyberbezpieczeństwa, w formie ankiety w Systemie Statystyki Ochrony Zdrowia przed przystąpieniem do działań mających na celu podniesienie poziomu bezpieczeństwa, finansowych w ramach niniejszego zarządzenia oraz przeprowadzenie audytu bezpieczeństwa zgodnie załącznikiem nr 2 do umowy.

6. Kwota finansowania dla jednego świadczeniodawcy nie może przekroczyć:

1) w przypadku złożenia przez świadczeniodawcę oświadczenia o możliwości odliczenia podatku VAT:

   a) 243 902 zł bez podatku VAT jeżeli suma wartości umów o udzielanie świadczeń opieki zdrowotnej, w rodzajach, o których mowa w niniejszej decyzji, zawartych przez danego świadczeniodawcę z Funduszem na 2021 r. jest nie większa niż 10 000 000 zł,

   b) 325 203 zł bez podatku VAT jeżeli suma wartości umów o udzielanie świadczeń opieki zdrowotnej, w rodzajach, o których mowa w niniejszej decyzji, zawartych przez danego świadczeniodawcę z Funduszem na 2021 r. jest większa od 10 000 000 zł i nie większa niż 100 000 000 zł,

   c) 487 804 zł bez podatku VAT jeżeli suma wartości umów o udzielanie świadczeń opieki zdrowotnej, w rodzajach, o których mowa w niniejszej decyzji, zawartych przez danego świadczeniodawcę z Funduszem na 2021 r. jest większa od 100 000 000 zł i nie większa niż 500 000 000 zł,

   d) 731 707 zł bez podatku VAT jeżeli suma wartości umów o udzielanie świadczeń opieki zdrowotnej, w rodzajach, o których mowa w niniejszej decyzji, zawartych przez danego świadczeniodawcę z Funduszem na 2021 r. jest większa od 500 000 000 zł;

2) w przypadku złożenia przez świadczeniodawcę oświadczenia o braku możliwości odliczenia podatku VAT:

   a) 300 000 zł z podatkiem VAT jeżeli suma wartości umów o udzielanie świadczeń opieki zdrowotnej, w rodzajach, o których mowa w niniejszej decyzji, zawartych przez danego świadczeniodawcę z Funduszem na 2021 r. jest nie większa niż 10 000 000 zł,

   b) 400 000 zł z podatkiem VAT jeżeli suma wartości umów o udzielanie świadczeń opieki zdrowotnej, w rodzajach, o których mowa w niniejszej decyzji, zawartych przez danego świadczeniodawcę z Funduszem na 2021 r. jest większa od 10 000 000 zł i nie większa niż 100 000 000 zł,

   c) 600 000 zł z podatkiem VAT jeżeli suma wartości umów o udzielanie świadczeń opieki zdrowotnej, w rodzajach, o których mowa w niniejszej decyzji, zawartych przez danego świadczeniodawcę z Funduszem na 2021 r. jest większa od 100 000 000 zł i nie większa niż 500 000 000 zł,

   d) 900 000 zł z podatkiem VAT jeżeli suma wartości umów o udzielanie świadczeń opieki zdrowotnej, w rodzajach, o których mowa w niniejszej decyzji, zawartych przez danego świadczeniodawcę z Funduszem na 2021 r. jest większa od 500 000 000 zł.

7. Koszty audytu bezpieczeństwa nie mogą przekroczyć 10 % wartości faktycznie udzielonego świadczeniodawcy finansowania.

8. W celu uzyskania finansowania, o którym mowa ust. 1, uprawniony świadczeniodawca, składa w terminie do 30 listopada 2022 r. do dyrektora właściwego oddziału Funduszu:

1) wniosek o zawarcie umowy na finansowanie ze środków pochodzących z Funduszu Przeciwdziałania COVID-19 podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców, zwany dalej „wnioskiem”, którego wzór określony jest w załączniku nr 1 do zarządzenia;

2) wypełnioną ankietę, o której mowa w ust. 3, badającą poziom bezpieczeństwa systemów teleinformatycznych w postaci raportu z Systemu Statystyki Ochrony Zdrowia, o którym mowa w ust. 6, sporządzonego w formacie pdf.

9. W przypadku, gdy świadczeniodawca posiada umowy o udzielanie świadczeń opieki zdrowotnej, o których mowa w § 1 ust. 2, realizowane na obszarze właściwości kilku oddziałów Funduszu, wniosek składa się dyrektora właściwego oddziału Funduszu, z którym została zawarta umowa o najwyższej wartości.

10. Dyrektor właściwego oddziału Funduszu w terminie 7 dni od dnia złożenia wniosku spełniającego warunki formalne, o których mowa w ust. 8, zawiera ze świadczeniodawcą umowę na finansowanie ze środków pochodzących z Funduszu Przeciwdziałania COVID-19 podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców, zwaną dalej „umową", której wzór określony jest w załącznik nr 2 do zarządzenia.

11. Informacja o wyniku rozpatrzenia wniosku o zawarcie umowy przekazywana jest świadczeniodawcy przez dyrektora właściwego oddziału Funduszu.

12. Wnioski złożone po terminie określonym w ust. 8 pozostawia się bez rozpatrzenia.

13. Warunkiem uzyskania przez świadczeniodawcę środków na finansowanie w wysokości maksymalnej określonej w ust. 6, jest zawarcie umowy i złożenie w siedzibie właściwego oddziału Funduszu nie później niż do 16 grudnia 2022 r. poniższych dokumentów:

1) wniosku o wypłatę finansowania, którego wzór określony jest w załączniku nr 3 do zarządzenia;

2) specyfikacji finansowania, której wzór określony jest w załączniku nr 4 do zarządzenia;

3) potwierdzonych za zgodność z oryginałem kopii dokumentów potwierdzających nabycie i sfinansowanie w okresie od dnia 29 kwietnia 2022 r. do dnia 31 grudnia 2022 roku przedmiotu finansowania, o którym mowa w ust. 1;

4) wynik audytu bezpieczeństwa, o którym mowa w ust. 3 i 5.

14. Środki, o których mowa w ust. 6, przekazywane są świadczeniodawcy, na rachunek wskazany w umowie, w terminie 14 dni od dnia złożenia w siedzibie właściwego oddziału Fundusz dokumentów, o których mowa w ust. 12, jednak nie później niż do 31 grudnia 2022 r. Za dzień zapłaty uważa się dzień obciążenia rachunku bankowego oddziału Funduszu.

Rozdział 3.
Rozliczenie środków na finansowanie

§ 4. 1. Dyrektor właściwego oddziału Funduszu w terminie do 10. dnia miesiąca następującego po miesiącu, w którym udzielono finansowania świadczeniodawcom na podstawie dokumentów, o których mowa w § 3 ust. 14, przekazuje do Centrali sprawozdanie miesięczne oraz narastająco, od pierwszego miesiąca do końca miesiąca, którego sprawozdanie dotyczy. Wzór sprawozdania określa załącznik nr 6 do zarządzenia.

2. Do sprawozdania, o którym mowa w ust. 1, za październik 2022 r., oddział Funduszu sporządza i przekazuje do Centrali prognozę wydatków na finansowanie działań, o których mowa w § 3 ust. 1 na okres listopad – grudzień 2022 r., sporządzoną na podstawie przewidywanych do poniesienia wydatków według wzoru określonego w załączniku nr 5 do zarządzenia.

3. Centrala Funduszu do 20. dnia miesiąca następującego po miesiącu, którego dotyczy sprawozdanie, o którym mowa w ust. 1, i prognoza, o której mowa w ust. 2, przekazuje na rachunek bankowy oddziału Funduszu środki finansowe w wysokości wynikającej ze złożonych sprawozdań i prognoz.

4. W terminie do dnia 6 stycznia 2023 r oddział Funduszu sporządza i przekazuje do Centrali sprawozdanie za grudzień 2022 roku.

5. W przypadku niewykorzystania środków, o których mowa ust. 3, oddział Funduszu dokonuje ich zwrotu w terminie do 6 stycznia 2023 r.

6. W przypadku konieczności dokonania korekty sprawozdania za miesiąc, za który sprawozdanie zostało uznane za sporządzone prawidłowo, korekty dokonuje się w sprawozdaniu sporządzanym w okresie stwierdzenia konieczności dokonania korekty, w części przedstawiającej dane narastające od pierwszego miesiąca do końca miesiąca, którego sprawozdanie dotyczy.

7. Oddział Funduszu zobowiązany jest do prowadzenia wyodrębnionej ewidencji księgowej dla zadania, o którym mowa w zarządzeniu, zgodnie z ustawą z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2021 r. poz. 217, z późn. zm.), w sposób umożliwiający identyfikację poszczególnych operacji księgowych w ramach realizacji zadania.

8. Sprawozdania oraz prognozy:

1) sprawdza pod względem merytorycznym i podpisuje kierownik Zespołu Bezpieczeństwa Informacji i Ciągłości Działania oddziału Funduszu albo osoba upoważniona przez dyrektora oddziału Funduszu;

2) sprawdza pod względem formalno – rachunkowym i podpisuje naczelnik Wydziału Księgowości – główny księgowy oddziału Funduszu albo osoba upoważniona przez dyrektora oddziału Funduszu;

3) zatwierdza dyrektor oddziału Funduszu albo osoba przez niego upoważniona

§ 5. 1. Centrala Funduszu, na podstawie sprawozdań oddziałów Funduszu, sporządza sprawozdania łączne, których wzór stanowi załącznik nr 6 do zarządzenia.

2. Informacje zawarte w sprawozdaniach, o którym mowa w ust. 1, wykazuje się odrębnie za miesiąc oraz narastająco.

3. Sprawozdanie, o którym mowa w ust. 1, sporządzone na podstawie danych otrzymanych z oddziałów Funduszu:

1) sprawdza pod względem zgodności z danymi przesłanymi z oddziałów wojewódzkich Funduszu i podpisuje kierownik Działu Rozliczeń Międzyoddziałowych i Dotacji Pozyskiwanych z Unii Europejskiej oraz Budżetu Państwa w Biurze Księgowości lub osoba zastępująca;

2) sprawdza pod względem merytorycznym i podpisuje dyrektor Biura Bezpieczeństwa Informacji i Ciągłości Działania Centrali Funduszu lub osoba zastępująca;

3) sprawdza pod względem formalno–rachunkowym i podpisuje dyrektor Biura Księgowości – Główny Księgowy Centrali Funduszu lub osoba zastępująca;

4) zatwierdza Prezes Funduszu lub osoba przez niego upoważniona.

4. Prezes Funduszu przekazuje ministrowi właściwemu do spraw zdrowia sprawozdanie, o którym mowa w ust. 1, w terminie do 20. dnia każdego miesiąca za miesiąc poprzedni.

5. W przypadku konieczności dokonania korekty sprawozdania za miesiąc, za który sprawozdanie zostało uznane za sporządzone prawidłowo, korekty dokonuje się w sprawozdaniu sporządzanym w okresie stwierdzenia konieczności dokonania korekty, w części przedstawiającej dane narastające od pierwszego miesiąca do końca miesiąca, którego sprawozdanie dotyczy.

6. Prezes Funduszu w terminie do 13 stycznia 2023 r. przekazuje ministrowi właściwemu do spraw zdrowia końcowe rozliczenie otrzymanych i wykorzystanych w 2022 r. środków.

7. W przypadku niewykorzystania otrzymanych środków do 31 grudnia 2022 r., Prezes Funduszu zwraca niewykorzystane środki ministrowi właściwemu do spraw zdrowia, w terminie do 13 stycznia 2023 r.Bernar

8. Za datę zwrotu środków, o których mowa w ust. 7, przyjmuje się dzień uznania rachunku ministra właściwego do spraw zdrowia.

§ 6. Zarządzenie wchodzi w życie z dniem następującym po dniu podpisania.

PREZES
NARODOWEGO FUNDUSZU ZDROWIA
Bernard Waśko

wz. Prezesa Narodowego Funduszu Zdrowia
/Dokument podpisano elektronicznie/

Załącznik Nr 1 do zarządzenia Nr 68/2022/BBIiCD

Prezesa Narodowego Funduszu Zdrowia

z dnia 20 maja 2022 r.

Wniosek o zawarcie umowy na finansowanie ze środków pochodzących z Funduszu Przeciwdziałania COVID-19 podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców

I. DANE IDENTYFIKACYJNE UPRAWNIONEGO ŚWIADCZENIODAWCY

Nazwa			
Adres siedziby			
REGON		NIP	

II. NUMERY UMÓW O UDZIELANIE ŚWIADCZEŃ

Numer umowy	Rodzaj świadczenia

III. NUMER RACHUNKU BANKOWEGO ŚWIADCZENIODAWCY, NA KTÓRY PRZEKAZANE ZOSTANĄ ŚRODKI

Dane posiadacza rachunku bankowego	
Numer rachunku bankowego	

IV. OŚWIADCZENIE

Oświadczam, że:

1) spełniam warunki do otrzymania finansowania określone w Zarządzeniu Prezesa Narodowego Funduszu Zdrowia w sprawie warunków udzielania i rozliczania finansowania podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców

2) mam / nie mam*) możliwości odliczenia podatku VAT (w rozumieniu przepisów ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. z 2022 r. poz. 931, z późn. zm.)

…… Miejscowość i data

……. Podpis świadczeniobiorcy

*) niepotrzebne skreślić

Załącznik Nr 2 do zarządzenia Nr 68/2022/BBIiCD

Prezesa Narodowego Funduszu Zdrowia

z dnia 20 maja 2022 r.

UMOWA Nr ..... /.....

o finansowanie ze środków pochodzących z Funduszu Przeciwdziałania COVID-19 podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców

zawarta w ....., dnia ..... roku, pomiędzy:

Narodowym Funduszem Zdrowia - …….....

(adres),

reprezentowanym przez Dyrektora ……

.....,

zwanego dalej **„Oddziałem Funduszu”,**

a

.....

.....

oznaczenie świadczeniodawcy: nazwa świadczeniodawcy w rozumieniu art. 5 pkt 41 ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. z 2021 r. poz. 1285, z późn. zm.), będącego podmiotem leczniczym, o którym mowa w art. 4 ust. 1 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz. U. z 2022 r. poz. 633, z późn. zm.) i prowadzącym szpital

zwanym dalej **„Świadczeniodawcą”**, reprezentowanym przez:

.....

PRZEDMIOT UMOWY

§ 1. 1. Przedmiotem umowy jest finansowanie ze środków pochodzących z Funduszu Przeciwdziałania COVID-19 działań w celu do podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawcy.

2. Świadczeniodawca zobowiązany jest wykonywać umowę z należytą starannością oraz zgodnie z postanowieniami zarządzenia Prezesa Narodowego Funduszu Zdrowia w sprawie finansowania podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców, zwanego dalej „zarządzeniem”.

WARUNKI FINANSOWANIA

§ 2. 1. Fundusz finansuje działania w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych u świadczeniodawców, wykonane przez świadczeniodawcę w ramach realizacji umowy, w okresie od dnia …… .2022 r. do dnia 31 grudnia 2022 r. do określonej zgodnie z § 3 ust. 6 zarządzenia kwoty, wynoszącej maksymalnie ……zł (słownie złotych: ……).

2. Ustalenie faktycznej kwoty finansowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawcy nastąpi po przedłożeniu przez świadczeniodawcę wniosku o wypłatę finansowania, specyfikacji finansowania, dokumentów potwierdzających nabycie i sfinansowanie wydatków oraz ich wysokość.

3. Finansowanie działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych u świadczeniodawców następuje zgodnie z zasadami określonymi w zarządzeniu.

4. Finansowanie, o którym mowa w ust. 3, następuje po wykazaniu przez świadczeniodawcę wynikiem audytu bezpieczeństwa potwierdzającego zwiększenie poziomu bezpieczeństwa teleinformatycznego u świadczeniodawcy, przeprowadzonym zgodnie z załącznikiem nr 2 do umowy.

5. Należność z tytułu realizacji zawartej umowy oddział Funduszu wypłaca na rachunek bankowy:

dane posiadacza rachunku bankowego:……

nr:……

6. Zmiana numeru rachunku bankowego, o którym mowa w ust. 3, wymaga uprzednio złożenia przez świadczeniodawcę, w formie pisemnej, wniosku w sprawie zmiany rachunku bankowego, którego wzór stanowi załącznik nr 1 do umowy.

OKRES OBOWIĄZYWANIA UMOWY

§ 3. 1. Umowa obowiązuje do 31 grudnia 2022 r., z zastrzeżeniem postanowień umownych wykraczających poza ten okres.

2. Należność z tytułu realizacji zawartej umowy oddział Funduszu wypłaca na rachunek bankowy nie później niż 31 grudnia 2022 r.

3. Zmiana postanowień umowy może nastąpić wyłącznie za zgodą Stron, poprzez zawarcie aneksu, w formie pisemnej, pod rygorem nieważności.

4. Stwierdzenie przez Fundusz nienależytego wykonywania umowy może stanowić podstawę do rozwiązania umowy bez wypowiedzenia w trybie natychmiastowym.

5. Każda ze stron może rozwiązać umowę za 7 dniowym okresem wypowiedzenia.

POSTANOWIENIA KOŃCOWE

§ 4. 1. W okresie od dnia zawarcia umowy do 31 grudnia 2027 r. Fundusz oraz Minister Zdrowia są uprawnieni do kontroli prawidłowości dokonywania przez świadczeniodawcę rozliczeń merytorycznych i finansowych wynikających z umowy i przyznanego finansowania, w szczególności w zakresie:

1) zgodności realizowanych działań z działaniami określonymi w zarządzeniu;

2) legalności i celowości wykorzystania finansowania przez świadczeniodawcę;

3) sposobu i rodzaju prowadzenia dokumentacji, określonej w przepisach szczególnych oraz zarządzeniu;

4) oceny prawidłowości dokonywania przez świadczeniodawcę rozliczeń merytorycznych i finansowych wynikających z zarządzenia i przyznanego finansowania.

2. W przypadku stwierdzenia wykorzystywania przyznanego finansowania niezgodnie z zarządzeniem i postanowieniami umowy, świadczeniodawca zwróci na rachunek bankowy Oddziału Funduszu otrzymane środki publiczne wydatkowane w sposób nieprawidłowy, w terminie 15 dni od dnia doręczenia wezwania do zwrotu wraz z odsetkami ustawowymi za opóźnienie naliczonymi od dnia otrzymania środków publicznych do dnia zwrotu na rachunek bankowy Oddziału Funduszu.

§ 5. Sądami właściwymi do rozpoznawania spraw spornych między stronami umowy są sądy powszechne właściwe dla Oddziału Funduszu.

§ 6. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

Świadczeniodawca	**Dyrektor Oddział Funduszu**
……	**…….**

Załączniki do umowy:

1) Wniosek w sprawie zmiany rachunku bankowego;

2) Wymagania dotyczące audytu bezpieczeństwa;

Załącznik nr 1 do umowy

Kod Oddziału Wojewódzkiego

Dane Świadczeniodawcy

Wniosek w sprawie zmiany rachunku bankowego

Wnoszę o podpisanie aneksu do istniejącej umowy o finansowanie ze środków pochodzących z Funduszu Przeciwdziałania COVID-19 podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców nr……., zmieniającego nr rachunku bankowego wskazany w zawartej umowie.
Nowy pełny numer rachunku bankowego związanego z realizacją umowy:
Dane posiadacza rachunku bankowego:

Zmiana dotychczasowego nr rachunku bankowego na nowy nastąpi po podpisaniu aneksu do umowy w terminie określonym w aneksie.

…… Miejscowość i data

……. Podpis świadczeniodawcy/osoby upoważnionej do reprezentowania świadczeniodawcy

Załącznik nr 2 do umowy

Wymagania dotyczące audytu bezpieczeństwa

Audyt bezpieczeństwa, o którym mowa w niniejszego zarządzenia może być przeprowadzony przez:

1) jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 5), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych;
2) co najmniej dwóch audytorów posiadających:
   a) certyfikaty określone w poniższym wykazie certyfikatów uprawiających do przeprowadzenia audytu lub
   b) co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, lub
   c) co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymujących się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych.

Wykaz certyfikatów uprawniających do przeprowadzenia audytu:

1. Certified Internal Auditor (CIA);

1) Certified Information System Auditor (CISA);
2) Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami *ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku,* w zakresie certyfikacji osób;
3) Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami *ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku*, w zakresie certyfikacji osób;
4) Certified Information Security Manager (CISM);
5) Certified in Risk and Information Systems Control (CRISC);
6) Certified in the Governance of Enterprise IT (CGEIT);
7) Certified Information Systems Security Professional (CISSP);
8) Systems Security Certified Practitioner (SSCP);
9) Certified Reliability Professional;
10) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

Celem audytu jest wykazanie przez świadczeniodawcę podniesienia poziomu bezpieczeństwa teleinformatycznego po zrealizowaniu czynności, zgodnie z niniejszym zarządzeniem oraz w odniesieniu do stanu na dzień przeprowadzenia badania poziomu dojrzałości cyberbezpieczeństwa u świadczeniodawcy w formie ankiety. Przeprowadzony audyt wykaże podniesienie poziomu bezpieczeństwa teleinformatycznego w odniesieniu do poziomu wynikającego z ankiety lub jego brak. Raport musi zawierać jasne stanowisko audytora w zakresie wykazania, że spożytkowane środki wpłynęły na podniesienie poziomu bezpieczeństwa.

Nazwa obszaru	Opis działań skutkujących podniesieniu poziomem bezpieczeństwa teleinformatycznego u świadczeniodawców
Skuteczność działania infrastruktury	-Urządzenia i konfiguracja w zakresie ochrony poczty -Urządzenia i konfiguracja w zakresie ochrony sieci -Urządzenia i konfiguracja w zakresie systemów serwerowych -Urządzenia i konfiguracja w zakresie stacji roboczych -Urządzenia i konfiguracja w zakresie systemów bezpieczeństwa
Procesy zarządzania bezpieczeństwem informacji	-Nośniki wymienne - udokumentowany sposób postępowania -Zarządzanie tożsamością / dostęp do systemów w zakresie: -- Przydzielanie dostępu -- Odbieranie dostępu -Pomieszczenie w dyspozycji struktur zespołu odpowiedzialnego za cyberbezpieczeństwo w przypadku podmiotów, które otrzymały decyzję uznającą taki podmiot za operatora usługi kluczowej, o którym mowa w art. 5 *ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa*
Monitorowanie i reagowanie na incydenty bezpieczeństwa	-Procedury zarządzania incydentami -Raportowanie poziomów pokrycia scenariuszami znanych incydentów -Dokumentacja dotycząca przekazywania informacji do właściwego zespołu CSIRT poziomu krajowego/ sektorowego zespołu cyberbezpieczeństwa -Monitorowanie i wykrycie incydentów bezpieczeństwa -Identyfikacja i dokumentowanie przyczyn wystąpienia incydentów
Zarządzanie ciągłością działania	-Konfiguracja oraz polityki systemów do wykonywania kopii bezpieczeństwa -Raport z przeglądów i testów odtwarzania kopii bezpieczeństwa -Procedury wykonywania i przechowywania kopii zapasowych -Strategia i polityka ciągłości działania, awaryjne oraz odtwarzania po katastrofie (DRP) -Procedury utrzymaniowe
Utrzymanie systemów informacyjnych	-Harmonogramy skanowania podatności -Aktualny status realizacji postępowania z podatnościami -Procedury związane ze z identyfikowaniem (wykryciem) podatności -Współpraca z osobami odpowiedzialnymi za procesy zarządzania incydentami

Zarządzanie bezpieczeństwem i ciągłością działania łańcucha usług	-Polityka bezpieczeństwa w relacjach z dostawcami -Standardy i wymagania nakładane na dostawców w umowach w zakresie cyberbezpieczeństwa -Dostęp zdalny -Metody uwierzytelnienia

Załącznik Nr 3 do zarządzenia Nr 68/2022/BBIiCD

Prezesa Narodowego Funduszu Zdrowia

z dnia 20 maja 2022 r.

Wniosek o wypłatę finansowania

I. DANE IDENTYFIKACYJNE UPRAWNIONEGO ŚWIADCZENIODAWCY

Nazwa			
Adres siedziby			
REGON		NIP	
Data i numer umowy o finansowanie ze środków pochodzących z Funduszu Przeciwdziałania COVID-19 podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców			

II. KWOTA WNIOSKOWANEGO FINANSOWANIA

zł	Słownie złotych:

III. OŚWIADCZENIE

Oświadczam, że:

1) wydatki poniesione na zwiększenie poziomu bezpieczeństwa teleinformatycznego objęte niniejszym wnioskiem zostały poniesione na warunkach określonych w Zarządzeniu Prezesa Narodowego Funduszu Zdrowia w sprawie warunków udzielania i rozliczania finansowania podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców;
2) wydatki poniesione na zwiększenie poziomu bezpieczeństwa teleinformatycznego objęte niniejszym wnioskiem (w tym zakupów urządzeń, oprogramowania, licencji, usług IT) nie były objęte finansowaniem z jakichkolwiek innych środków publicznych zewnętrznych, w tym krajowych bądź europejskich (wykluczenie podwójnego finansowania).

IV. ZOBOWIĄZANIE

Zobowiązuję się do:

1) wykorzystania finansowania działań doprowadzających do podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawcy wyłącznie na cele wskazane w zarządzeniu Prezesa Narodowego Funduszu Zdrowia w sprawie warunków udzielania i rozliczania dofinansowania podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców. Za wykorzystanie przyznanych środków rozumie się zakup, zapłatę oraz odbiór urządzeń informatycznych lub oprogramowania lub usług;
2) stosowania procedur zawierania umów wynikających z ustawy z dnia 29 stycznia 2004 r. - Prawo zamówień publicznych (Dz. U. 2021 r. poz. 1129, z późn. zm.), chyba że świadczeniodawca nie jest zamawiającym w rozumieniu tej ustawy;
3) przechowywania dokumentacji związanej z udzieleniem finansowania, w tym dowodów zakupu lub wykonania usługi, przez okres co najmniej pięciu lat począwszy od 1 stycznia 2023 r., chyba że przepisy powszechnie obowiązujące przewidują dłuższy okres przechowywania dokumentacji.

…… …….

Miejscowość i data Podpis świadczeniobiorcy

Załącznik Nr 4 do zarządzenia Nr 68/2022/BBIiCD
Prezesa Narodowego Funduszu Zdrowia
z dnia 20 maja 2022 r.

Specyfikacja finansowania

Specyfikacja finansowania

w złotych

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
L p.	Nazwa świadczeniodawcy	NIP świadczeniodawcy	Czy podmiot ma możliwość odliczenia VAT (TAK/NIE) *	Faktura						Data: odbioru urządzenia informatycznego lub oprogramowania wykonania usługi**	Wartość kwalifikująca się do finansowania	Wnioskowana kwota finansowania	Producent oprogramowania	Nazwa oprogramowania	Wersja oprogramowania	Nazwa urządzenia informatycznego	Nazwa usługi	Uwagi
				Numer	Data wystawienia (rrrr-mm-dd)	Termin płatności (rrrr-mm-dd)	Wartość netto	Wartość brutto	Data zapłaty faktury (rrrr-mm-dd)									
1																		
2																		
3																		
Razem:																		

* należy wpisać TAK w przypadku możliwości odliczenia VAT, NIE w przypadku braku możliwości odliczenia VAT
** jeden wiersz może dotyczyć tylko jednej pozycji zakupowej FV zadeklarowanej do dofinansowania, w przypadku kilku pozycji zakupowych FV należy uzupełnić każdy wiersz osobno dla każdej pozycji zakupowej FV

Miejscowość i data:

Imię i nazwisko Sporządzającego:

Nr telefonu:

Adres e-mail:

……
……
Podpis
osoby upoważnionej
do reprezentowania świadczeniodawcy

Załącznik Nr 5 do zarządzenia Nr 68/2022/BBIiCD
Prezesa Narodowego Funduszu Zdrowia
z dnia 20 maja 2022 r.

Prognoza wydatków z tytułu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców

Lp.	Oddział wojewódzki NFZ	Prognozowana kwota finansowania w listopadzie 2022 r.	Prognozowana kwota finansowania w grudniu 2022 r.	Uwagi
1				

Miejscowość i data:

Imię i nazwisko Sporządzającego:

Nr telefonu:

Adres e-mail:

.....	.....	.....
Naczelnik komórki odpowiedzialnej merytorycznie za realizację zarządzenia albo osoba upoważniona	**Naczelnik Wydziału Księgowości Główny Księgowy OW NFZ albo osoba upoważniona**	**Dyrektor OW NFZ albo osoba upoważniona**

Załącznik Nr 6 do zarządzenia Nr 68/2022/BBIiCD
Prezesa Narodowego Funduszu Zdrowia
z dnia 20 maja 2022 r.

Sprawozdanie za miesiąc …… 2022/ za okres od…… do …….. 2022 r.

Lp.	Nazwa świadczeniodawcy	NIP świadczeniodawcy	Przedmiot finansowania				Razem kwota finansowania	Wnioskowana kwota finansowania
			Sprzęt informatyczny	Usługi informatyczne	Oprogramowanie/licencje	Usługi szkoleniowe		
1	2	3	4	5	6	7	8=4+5+6+7	9
1								
2								
3								
Razem:								

Miejscowość i data:

Imię i nazwisko sporządzającego:

Nr telefonu:

Adres e-mail:

Sprawdzono pod względem merytorycznym

Sprawdzono pod względem formalno - rachunkowym

Zatwierdził

Uzasadnienie

Zgodnie z treścią art. 11h ust. 2 pkt 2 i ust. 4 ustawy z dnia z 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID- 19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz. U. z 2021 r. poz. 2095, z późn. zm.) w okresie ogłoszenia stanu zagrożenia epidemicznego lub stanu epidemii, ogłoszonego z powodu COVID-19, oraz w okresie 3 miesięcy po ich odwołaniu minister właściwy do spraw zdrowia może, z własnej inicjatywy lub na wniosek wojewody, wydawać, w formie decyzji administracyjnej, polecenia obowiązujące państwowe jednostki organizacyjne posiadające osobowość prawną.

Wykorzystanie usług e-zdrowia w pandemii COVID-19 miało kluczowe znaczenie w sektorze ochrony zdrowia i wskazuje się na trwałą potrzebę zastosowania takich rozwiązań. Również w akcie prawnym istotnym z punktu widzenia epidemii COVID-19, tj. rozporządzeniu Rady Ministrów z dnia 25 marca 2022 r. w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii, wskazano na konieczność podejmowania czynności w trakcie udzielania świadczeń opieki zdrowotnej za pośrednictwem systemów teleinformatycznych lub systemów łączności.

System opieki zdrowotnej w Polsce od dłuższego czasu podlegał intensywnej transformacji cyfrowej. Głównym celem przedmiotowego procesu było szukanie rozwiązań gwarantujących zwiększenie wydajności systemu, jego bezpieczeństwa, a tym samym skuteczności. Niewątpliwie trwająca w Polsce epidemia znacznie przyspieszyła ten proces i przełożyła się na zwiększenie liczby świadczeń opieki zdrowotnej udzielanych za pośrednictwem systemów teleinformatycznych lub systemów łączności. Pandemia spowodowała trwały wzrost korzystania przez pacjentów z usług e-zdrowia jak i środków komunikacji elektronicznej. Zatem popularyzacja telemedycyny, usług e-zdrowia, jako usług które będą się stale rozwijać, a także doświadczenia z tym związane zdobyte w czasie pandemii uzasadniają wprowadzanie rozwiązań mających na celu zabezpieczenia realizacji tych usług w systemach teleinformatycznych. Należy bowiem mieć na uwadze, że korzystanie z systemów teleinformacyjnych jak i środków komunikacji elektronicznej nierozerwalnie związane jest z możliwością wystąpienia incydentu, w tym incydentu mogącego wpłynąć na zaistnienie szkody czy też uniemożliwienie prowadzenia działalności leczniczej.

W systemie ochrony zdrowia incydenty w zakresie cyberbezpieczeństwa, w okresie ostatnich 2 lat występowały zdecydowanie częściej. Takie incydenty jak wyciek danych w tym danych osobowych pacjentów, blokowanie systemu i szyfrowanie plików wraz z żądaniami okupu są coraz częstszym zjawiskiem, również w Polsce. Mogą one prowadzić do paraliżu i ogromnych strat podmiotach leczniczych oraz zagrozić życiu i zdrowiu pacjentów. Incydenty cyberbezpieczeństwa mogą skutecznie uniemożliwić przeprowadzanie planowanych operacji czy zagrozić prywatności danych osobowych, w szczególności danych wrażliwych pacjentów. Jak wynika z danych CERT Polska w ostatnim czasie odnotowano wzrost liczby ataków złośliwego oprogramowania typu ransomware w wielu sektorach gospodarki, w tym w sektorze ochrona zdrowia. W 2019 roku w Polsce zarejestrowano 53 incydenty cyberbezpieczeństwa dotyczące sektora ochrony zdrowia, a od 1 stycznia 2020 roku do września 2020 roku odnotowano ich już ponad 90. Podczas trwania epidemii COVID-19 Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) zaobserwowała znaczny wzrost incydentów - o 47 %, a według Check Point Research cyberprzestępcy coraz częściej kierują swoje ataki przeciw szpitalom głównie w Europie Środkowej. Na całym świecie odnotowano w 2021 r. znaczny wzrost incydentów cyberbezpieczeństwa skierowanych głównie na szpitale aż o 71 proc. w porównaniu z rokiem 2020.

Mając na uwadze powyższe należy wskazać na wciąż trwające niebezpieczeństwo wystąpienia incydentów cyberbezpieczeństwa, co stanowi trwały skutek społeczno- gospodarczy pandemii COVID-19 W związku z tym niezbędne jest dalsze odpowiedzialne i szerokie zabezpieczanie wszystkich systemów teleinformatycznych w podmiotach leczniczych, co może być możliwe dzięki zapewnieniu odpowiedniego finansowana w tym zakresie. Podmioty lecznicze prowadzące szpitale znajdowały się na pierwszej linii walk z chorobą COVID-19 i dalej zagrożone jest ich bezpieczeństwo. Tym samym ogromne znaczenie ma ochrona systemów informatycznych wykorzystywanych przez te podmioty do udzielania świadczeń opieki zdrowotnej.

Minister Zdrowia kierując się skutkami społeczno-gospodarczymi pandemii COVID-19, podjął decyzję o nałożeniu obowiązków na NFZ w tym zakresie, w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców wykorzystywanych do udzielania świadczeń opieki zdrowotnej. Należy mieć przy tym na uwadze, że celem przedmiotowej decyzji jest zapewnienie zwiększenia poziomu bezpieczeństwa systemów teleinformatycznych z uwagi na zwiększenie częstotliwości podatności tych systemów na incydenty cyberbezpieczeństwa na skutek pandemii COVID-19, a nie informatyzacja

świadczeniodawców, której celem jest udzielanie przez nich świadczeń opieki zdrowotnej za pośrednictwem systemów teleinformatycznych lub systemów łączności, prowadzenie i wymiana elektronicznej dokumentacji medycznej, w tym digitalizacja dokumentacji medycznej prowadzonej w postaci papierowej oraz udostępnianie elektronicznych usług świadczeniobiorcom lub innym podmiotom. Zatem działania wskazane w niniejszej decyzji należy odróżnić od zadania NFZ, o którym mowa w art. 97 ust. 3 pkt 4c ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. z 2021 r. poz. 1285, z późn. zm.).