Załącznik nr 7 do SWKO

UMOWA O OCHRONIE DANYCH
(Umowa powierzenia przetwarzania danych osobowych)

zawarta pomiędzy Administratorem i Podmiotem Przetwarzającym
DD.09210.....2022

Umowa powierzenia przetwarzania danych osobowych, (dalej jako Umowa) na podstawie art. 28 ust. 3 Rozporządzenia Parlamentu Europejskiego i Rady 2016/679 (Rozporządzenie o ochronie danych osobowych) w związku z przetwarzaniem danych osobowych przez podmiot przetwarzający zawarta pomiędzy:

Szpitalem Wojewódzkim im. M. Kopernika w Koszalinie, ul. Chałubińskiego 7, 75-581 Koszalin, reprezentowanym przez Andrzeja Kondaszewskiego - Dyrektora, zwanym w dalszej części umowy **„Administratorem"**

a

.....

zwanym dalej **„Podmiotem przetwarzającym"**

zwani dalej łącznie : Stronami, a każda z osobna Stroną.

Niniejsza Umowa pełni rolę uzupełnienia do wszystkich umów, dotyczących udzielania świadczeń w zakresie nocnej i świątecznej opieki zdrowotnej zawartych pomiedzy Stronami. Mając na uwadze, iż:

a) sposób przetwarzania danych polegać będzie w szczególności na wykonywaniu czynności niezbędnych dla celów realizacji umów, dotyczących świadczeń opieki zdrowotnej w zakresie nocnej i świątecznej opieki zdrowotnej, udzielanych w warunkach ambulatoryjnych oraz w miejscu zamieszkania lub pobytu świadczeniobiorcy,
b) udzielanie świadczeń opieki zdrowotnej w zakresie nocnej i świątecznej opieki zdrowotnej wymaga i jest uzależnione od dostępu Podmiotu przetwarzajacego do bazy danych Administratora w systemie informatycznym ESKULAP,
c) udzielanie świadczeń w zakresie nocnej i świątecznej opieki zdrowotnej wymaga rejestrowania rozmów telefonicznych,
d) w odniesieniu postanowień zawartych pomiędzy Stronami, w tym: w odniesieniu do zmian, poprawek i aneksów oraz wszystkich powiązanych z nimi porozumień umownych, a także dla uniknięcia wątpliwości Udzielajacy zamówienia pełni rolę Administratora danych, Przyjmujący zamówienie pełni rolę Podmiotu przetwarzającego.
e) strony zawierając Umowę o ochronie danych dążą do takiego uregulowania zasad przetwarzania danych osobowych, aby odpowiadały one w pełni przepisom 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 (Dz. Urz. UE L 119, s. 1) zwane dalej rozporzadzeniem o ochronie danych,

Strony zgodnie postanawiają, co następuje:

§ 1

Załączniki

1. Do Umowy o ochronie danych dołączone są cztery Załączniki, które stanowią integralną część postanowień tej Umowy. Każda zmiana Załącznika wymaga akceptacji Stron.
    a) Załącznik A zawiera informacje na temat przetwarzania danych osobowych, w tym informacje dotyczace celu i charakteru przetwarzania, rodzaju danych osobowych, kategorii osób, których dane dotyczą oraz czasu trwania przetwarzania.
    b) Załącznik B zawiera warunki dotyczące korzystania przez Podmiot przetwarzający z Podwykonawców przetwarzających dane oraz wykaz podwykonawców, których Administrator zatwierdził.
    c) Załącznik C zawiera informacje dotyczące środków bezpieczeństwa, oraz sposób przeprowadzania przez Administratora audytów u Podmiotu przetwarzającego i podwykonawców.
    d) Załącznik D zawiera postanowienia dotyczące zasad dostępu do: systemu informatycznego Eskulap, zasad udostępniania zarejestrowanych nagrań telefonicznych.
2. Umowa o ochronie danych wraz z Załącznikami będzie przechowywana przez obie Strony w formie pisemnej, w tym w formie elektronicznej.
3. Strony zobowiązują się nie zmieniać postanowień zawartych w niniejszej Umowie z wyjątkiem dodawania informacji do Załączników, lub aktualizowania zawartych w nich informacji.
4. Wszelkie zmiany w Załącznikach nie mogą być bezpośrednio lub pośrednio sprzeczne z niniejszymi postanowieniami, i nie mogą naruszać podstawowych praw lub wolności osób, których dane dotyczą.
5. Jeżeli w Umowie o ochronie danych użyto terminów zdefiniowanych odpowiednio w rozporządzeniu (UE) 2016/679 lub rozporządzeniu (UE) 2018/1725, terminy te mają takie samo znaczenie, jak w tych rozporządzeniach.
6. Przetwarzanie danych przez Podmiot przetwarzający odbywa się wyłącznie przez okres określony w Załączniku A.

§ 2

Poufność przetwarzania

1. Strony oświadczają, że dane osobowe powierzone do przetwarzania na podstawie niniejszej Umowy i wszelkie informacje, o których Strony uzyskają wiadomość w związku z zawarciem i wykonywaniem Umowy na udzielanie świadczeń zdrowotnych są poufne, posiadają wartość aktywów chronionych i co do swej istoty nie są jawne.
2. Dane osobowe stanowią informacje chronione tajemnicą zawodową osób wykonujących zawód medyczny, chronione ustawą o prawach pacjenta, rozporzadzeniu o ochronie danych i przepisami prawa powszechnie obowiązującego.
3. Obowiązek zachowania w tajemnicy danych osobowych/informacji nie dotyczy:
    a) obowiązku ujawniania, wynikającego z bezwzględnie obowiązujących przepisów prawa,
    b) druga Strona wyraziła zgodę na ich ujawnienie,
    c) stały się powszechnie znane wskutek okoliczności od Stron niezależnych,
    d) są niezbędne do świadczenia na rzecz każdej ze Stron usług przez podmioty zobowiązane do zachowania tajemnicy zawodowej, w szczególności biegłych rewidentów, radców prawnych.

§ 3

Bezpieczeństwo przetwarzania

1. Administrator danych ocenia zagrożenia dla praw i wolności osób fizycznych związane z przetwarzaniem, i podejmuje środki w celu zminimalizowania tych zagrożeń,
2. Podmiot przetwarzający niezależnie od Administratora ocenia również zagrożenia dla praw i wolności osób fizycznych związanych z przetwarzaniem, i podejmuje środki w celu zminimalizowania tych zagrożeń, mając na uwadze zapewnienie danym osobowym atrybutów: poufności, dostępności i integralności.

§ 4

Korzystanie z usług pomiotów podprzetwarzających (podwykonawców)

1. Jeżeli należyta realizacja obowiązków wynikających ze swiadczenia usług z Umowy o ochronie danych będzie tego wymagała, Podmiot przetwarzający może dokonać dalszego powierzenia przetwarzania danych osobowych na warunkach okreslonych w art. 28 ust. 2 i 4 Rozporządzenia o ochronie danych.
2. Warunkiem korzystania przez Podmiot przetwarzajacy z Podwykonawcy jest zgoda Administratora, z jednoczesnym oświadczeniem, że podmiot, któremu podpowierzono dane osobowe (podwykonawca przetwarzający dane) spełnia wymogi określone w art.28 RODO i zostanie to zagwarantowane w dalszej umowie powierzenia (umowie podpowierzenia).
3. W przypadku, gdy Podmiot przetwarzający uzyskał:
   a) konkretną pisemną zgodę Administratora, to składa wniosek o zatwierdzenie Podwykonawcy, w terminie określonym przez Administratora,
   b) ogólną zgodę Administratora, to powiadamia Administratora na piśmie o wszelkich planowanych zmianach dotyczących dodania lub zastąpienia Podwykonawców, w terminie określonym przez Administratora,

   uprawnienia podmiotu, któremu Podmiot przetwarzajacy powierzy dane osobowe nie mogą być szersze aniżeli uprawnienia, które Strona uzyskała w wyniku niniejszej Umowy.
4. W przypadku, gdy Podmiot przetwarzający korzysta z usług Podwykonawcy, wówczas Podmiot przetwarzajacy jest :
   a) odpowiedzialny za wymaganie od Podwykonawcy przestrzegania obowiązków Podmiotu przetwarzającego wynikajacych z niniejszej Umowy
   b) ponosi ponosi pełną odpowiedzialność wobec Administratora wynikającą z przepisów Rozporządzenia o ochronie danych, w szczególności z art. 79 i 82.
5. Kopia umowy o podwykonawstwo oraz wszelkie późniejsze zmiany są, przekazywane Administratorowi, w celu sprawdzenia czy Podwykonawca podlega tym samym obowiązkom, co do zakresu i ochrony danych osobowych, które określone zostały w niniejszej Umowie. Postanowienia handlowe, które nie wpływają na treść umowy o podwykonawstwo z zakresu ochrony danych osobowych, nie podlegają wymogowi przekazania kopii do Administratora.
6. Powiadomienia o wybraniu podwykonawcy Podmiot przetwarzajacy może dokonać w formie pisemnej lub elektronicznej.
7. Uprawnienie dotyczące powiadomienia o podmiocie przetwarzającym nie wyłącza możliwości wyrażenia sprzeciwu przez Administratora,
8. W przypadku wyrażenia sprzeciwu Podmiot przetwarzajacy dołoży staranności przy wyborze podwykonawcy i przeprowadzi proces weryfikacji pod kątem zgodności z prawem i bezpieczeństwa przetwarzania danych osobowych.

9. Uprawnienie do dalszego powierzania danych osobowych przez Przyjmującego zamówienie nie obejmuje przekazywania danych do państwa trzeciego, w rozumieniu art. 44 RODO. W takim wypadku wymagana jest zgoda Administratora.

§ 5

Pomoc dla Administratora

1. Podmiot przetwarzający zamówienie zobowiązany jest wspierać Administratora w wywiązywaniu się z obowiązków w zakresie bezpieczeństwa danych, zarządzania naruszeniem ochrony danych osobowych oraz ich zgłaszaniem do organu nadzoru oraz osoby, której dane dotyczą, oceny skutków dla ochrony danych oraz konsultacjami z organem nadzoru zgodnie z art.32-36 RODO.
2. Podmiot przetwarzajacy zobowiązany jest współpracować z Administratorem w zakresie udzielania odpowiedzi na żądanie osoby, której dane dotyczą, opisane w rozdziale III RODO.
3. W sytuacji wystąpienia zagrożeń mogących mieć wpływ na odpowiedzialność Administratora za przetwarzanie powierzonych danych osobowych Podmiot przetwarzajacy:
   a) zobowiązany jest niezwłocznie podjąć działania w celu ich usunięcia,
   b) pomaga Administratorowi w zgłoszeniu incydentu bezpieczenstwa,naruszenia ochrony danych właściwemu organowi nadzorczemu. Oznacza to, że Podmiot przetwarzający dane pomaga w uzyskaniu informacji, które zgodnie: z art. 33 pkt 3 rozporządzenia o ochronie danych Administrator przekazuje w zgłoszeniu naruszenia do właściwego organu nadzorczego, a w przypadku incydentu bezpieczeństwa zgodnie z art.11 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa Administrator jako operator usługi kluczowej przekazuje do własciwego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego.

§ 6

Odpowiedzialność

1. Podmiot przetwarzajacy jest odpowiedzialny w pełnej wysokości do pokrycia rzeczywistej szkody, jaką wyrządzi Administratorowi lub osobom trzecim w wyniku niezgodnego z niniejszą Umową i przepisami Rozporządzenia o ochronie danych przetwarzaniem danych osobowych, co nie wyłącza wyrównania Administratorowi poniesionej szkody.

§ 7

Usuwanie i zwrot informacji

1. Po zakończeniu świadczenia usług zgodnie z wyborem Administratora Podmiot przetwarzający:
   a) usunie wszystkie dane osobowe, które były przetwarzane w imieniu administratora danych i potwierdza administratorowi danych, że dane zostały usunięte
   b) lub zwróci wszystkie dane osobowe danych i usunie istniejące kopie, chyba że prawo Unii lub przepisy prawa polskiego będą wymagały przechowywania danych osobowych po zakończeniu świadczenia usług przez Podmiot przetwarzający.

§ 8

Audyt, w tym kontrole

Zasady prowadzenia audytu w tym kontroli określone zostały w Załączniku C.

§ 9

Hierarchia

1. W razie sprzeczności między niniejszymi postanowieniami a postanowieniami powiązanych umów zawartych między Stronami a istniejących w chwili uzgadniania niniejszych postanowień lub zawartych po ich uzgodnieniu, pierwszeństwo mają niniejsze postanowienia.

§ 10

Osoby kontaktowe u Administratora danych i Podmiotu przetwarzającego dane

1. Strony mogą kontaktować się ze sobą za pośrednictwem poniższych osób kontaktowych.
2. Strony zobowiązują się do informowania się na bieżąco o zmianach dotyczących osób kontaktowych:
   a) po stronie Administratora: Anna Kobusińska, Jolanta Gliwa – Inspektor Ochrony Danych, tel. 94 34 88 545 lub 94 34 88 151, adres e-mail: sekretariat@swk.med.pl
   b) po stronie Podmiotu przetwarzającego: [Imię i nzawisko] [STANOWISKO] [NUMER TELEFONU] [Adres e-mail].

§ 11

Wejście w życie i wypowiedzenie

1. Umowa o ochronie danych obowiązuje z dniem podpisania przez obie Strony.
2. Strony mogą żądać renegocjacji postanowień Umowy, jeżeli uzasadnią to zmiany przepisów prawa lub niezgodności w Umowie.
3. Umowa obowiązuje przez czas świadczenia usług przetwarzania danych.
4. W sprawach nieuregulowanych niniejszą Umową mają zastosowanie przepisy prawa polskiego.
5. Spory wynikłe z zastosowania tej Umowy rozpatrywane będą przez sąd właściwy dla siedziby Administratora.

W imieniu Administratora

W imieniu Podmiotu przetwarzającego

Załącznik A. Informacja o przetwarzaniu

Nr Załącznika	Wersja	Data aktualizacji	Nr Umowy Głównej	Wprowadzone zmiany	Czas trwania przetwarzania (czas trwania Umowy Głównej)
A.	0.1			Określone w pkt.od A1do A4	od.....do.....
A.	1.0				

[UWAGA: w przypadku kilku czynności przetwarzania informacje muszą być wypełnione dla każdej czynności przetwarzania]

A.1. Celem przetwarzania danych osobowych przez Podmiot przetwarzający w imieniu Administratora danych jest udzielanie świadczeń opieki zdrowotnej w zakresie nocnej i świątecznej opieki zdrowotnej, w warunkach ambulatoryjnych oraz w miejscu zamieszkania lub pobytu świadczeniobiorcy, w szczególności :

a) porad lekarskich ambulatoryjnych,
b) porad lekarskich udzielanych w miejscu zamieszkania lub pobytu świadczeniobiorcy,
c) porad lekarskich udzielonych telefonicznie,
d) świadczeń pielęgniarskich ambulatoryjnych,
e) świadczeń pielęgniarskich udzielanych w miejscu zamieszkania lub pobytu świadczeniobiorcy.

A.2. Przetwarzanie danych osobowych przez Podmiot przetwarzający w imieniu Administratora dotyczy przede wszystkim wprowadzania danych do dokumentacji medycznej w systemie informatycznym Eskulap.

A.3. Przetwarzanie obejmuje następujące rodzaje danych osobowych o osobach, których dane dotyczą: imię i nazwisko, adres e-mail, numer telefonu, adres, numer PESEL, dane dotyczace stanu zdrowia, inne dane niezbędne do realizacji udzielania świadczeń zdrowotnych.

A.4. Przetwarzanie obejmuje następujące kategorie osób, ktorych dane dotyczą: dane dotyczące pacjentów, osób upowaznionych przez pacjentów do dostepu do informacji/ do dokumentacji medycznej.

Załącznik B. Podwykonawcy przetwarzania

Nr Załącznika	Wersja	Data aktualizacji	Nr Umowy Głównej	Wprowadzone zmiany	Czas trwania powierzenia przetwarzania od..do...
B.	0.1			Określone w pkt od B1do B2	
	1.0				

B.1. Zawiadomienie o zatwierdzeniu podwykonawców przetwarzania

Termin zgłoszenia Administratorowi danych do zatwierdzenia podwykonawcy wynosi 14 dni.

Nr umowy podpowierzenia	Zgłoszony Podwykonawca	Data zgłoszenia Podwykonawcy przez Podmiot przetwarzajacy	Decyzja Administratora	Opis przetwarzania

B.2 Zatwierdzeni podwykonawcy przetwarzania

Administrator danych wyraża zgodę na korzystanie z następujących podmiotów przetwarzających dane:

Nr umowy podpowierzenia	Data zatwierdzenia Podwykonawcy przez Podmiot przetwarzajacy	Nazwa Podwykonawcy	Adres Podwykonawcy

Administrator danych wyraził zgodę na powierzenie danych osobowych ww. podprocesorom do czynności przetwarzania danych. Przetwarzający dane nie może - bez wyraźnej pisemnej zgody Administratora danych - wykorzystywać Podprzetwarzającego dane do innej czynności przetwarzania niż uzgodniona dla niego ani używać innego Podprzetwarzającego poddawanych danych do opisanej czynności przetwarzania.

Załącznik C. Polecenie przetwarzania - Instrukcja przetwarzania danych osobowych

Nr Załącznika	Wersja	Data aktualizacji	Nr Umowy Głównej	Wprowadzone zmiany	Czas trwania powierzenia przetwarzania od ..do..
C.	0.1			określone w pkt.od C1do C6	
	1.0				

C.1. Przedmiot przetwarzania danych/ instrukcja przetwarzania.

Podmiot przetwarzający, wykonuje następujące czynności przetwarzania:

a) udziela świadczeń zdrowotnych,
b) prowadzi dokumentację medyczną

C.2. Bezpieczeństwo informacji.

Przetwarzanie danych obejmuje dane osobowe pacjentów, dlatego wymagany jest wysoki poziom bezpieczeństwa.

Podmiot przetwarzajacy pomaga Administratorowi w wypełnianiu obowiązków wynikających z art. 32 rozporzadzenia o ochronie danych dostarczając niezbędnych informacji na temat podjetych środków zaradczych wobec zidentyfikowanych zagrożeń. Podmiot przetwarzający ma prawo podejmowania decyzji o tym, jakie techniczne i organizacyjne środki bezpieczeństwa należy wdrożyć w celu ustalenia niezbędnego poziomu bezpieczeństwa, jednakże jeśli w opini Administratora wymagane jest podjęcie dodatkowych środków Podmiot przetwarzający wdraża następujące środki, które zostały uzgodnione z Administratorem:

1. Wymagania dotyczące zachowania tajemnicy.
   Obowiązek zachowania w tajemnicy powierzonych danych – danych pacjentów, zarówno danych identyfikacyjnych i danych szczególnej kategorii wprowadzonych do dokumentacji papierowej i elektronicznej, informacje dotyczące sposobu zabezpieczania danych w systemie informatycznym Eskulap, sposobu zabezpieczania pomieszczeń, a także materiałów uzyskanych w związku z zawarciem i realizacją Umowy obejmuje wszystkich uczestników w trakcie i po realizacji niniejszej Umowy, w szczególności dotyczy; sposobów ich zabezpieczania, zakazu ujawniania w jakiejkolwiek formie treści informacji i udostępniania danych osobowych/informacji innym podmiotom, bez pisemnej zgody Administratora.

2. Wymagania szczególne dotyczące zachowania tajemnicy.
   Podmiot przetwarzajacy jak i jego pracownicy/ współpracownicy zobowiązani są do zachowania w tajemnicy danych osobowych/ informacji związanych z pacjentem, także po śmierci pacjenta.

3. Wymagania dotyczące dostępu do danych osobowych przetwarzanych w imieniu Administratora.
   Podmiot przetwarzający udziela dostępu do danych swoim pracownikom wyłącznie w niezbędnym zakresie i tylko tym osobom, które zobowiazane zostały do zachowania poufności lub podlegają odpowiedniemu ustawowemu obowiązkowi zachowania poufności. Podmiot przetwarzajacy prowadzi i na bieżaco sprawdza listę osób, którym przyznano dostęp do danych. Nadawanie uprawnień do systemu informatycznego Eskulap odbywa się wg procedury w Załączniku D.

4. Wymagania dotyczące pseudonimizacji i szyfrowania danych.
   Umowa nie przewiduje konieczności przesyłania danych. W przypadku nieprzewidzianym umową ze względu na szczególne okoliczności przesyłanie danych może odbywać się jedynie w niezbędnym zakresie przy zastosowaniu technik szyfrujących.

5. Wymagania dotyczące zapewnienia ciągłej poufności, dostępności i integralności systemów przetwarzania i usług.
   Podmiot przetwarzający zapewnia dostęp do danych tylko osobom upoważnionym, zapoznaje pracowników z konsekwencjami prawnymi wynikajacymi z utraty poufności danych pacjentów, zobowiązuje pracowników do przestrzegania procedur pracy w systemach informatycznych, zapoznaje pracowników z zagrożeniami.

6. Wymagania dotyczące możliwości przywrócenia dostępności do danych w systemie informatycznym.
   Zapewnienie ciągłości działania systemów informatycznych określone zostało w Polityce Zarządzania Ciagłością Działania - dokument Systemu Zarządzania Bezpieczeństwem Informacji.
7. Wymagania dotyczące procesów regularnego badania, oceny i oceny efektywności środków technicznych i organizacyjnych dotyczących zabezpieczenia bezpieczeństwa informacji osobowych.
   Przetwarzanie danych pacjentów wymaga regularnej oceny przez Pomiot przetwarzający zagrożeń związanych z przetwarzaniem i podejmowania środków w celu zminimalizowania tych zagrożeń.

8. Wymagania dotyczące dostępu do informacji przez internet.
   Umowa na udzielanie świadczeń zdrowotnych nie przewiduje dostepu do informacji przez internet.

9. Wymagania dotyczące ochrony informacji podczas przesyłania.
   Umowa na świadczenia zdrowotne nie przewiduje przesyłania danych na zewnątrz, tj. poza system informatyczny

10. Wymagania dotyczące ochrony informacji podczas przechowywania.
    Dokumentacja medyczna prowadzona jest w systemie informatycznym Eskulap. Dokumentacja medyczna prowadzona w formie papierowej wymaga zabezpieczeń przed nieuprawnionym udostępnieniem,np. przekazaniem osobie nieuprawnionej, zgubieniem lub zniszczeniem.

11. Wymagania dotyczące bezpieczeństwa fizycznego miejsc, w których przetwarzane są dane osobowe.
    W Szpitalu wyznaczone są trzy strefy bezpieczeństwa: ogólnodostępna, administracyjna, chroniona. Prawo wejścia do steref chronionych maja tylko pracownicy, którym wydano uprawnienia dostepu do pomieszczeń. Przebywanie w strefie chronionej osób nieuprawnionych mozliwe jest tylko w obecnosci osoby uprawnionej.

12. Wymagania dotyczące pracy poza siedzibą.
    Pracownicy zobowiązani są do ochrony informacji podczas transportu i wykonywania świadczeń medycznych.

13. Wymagania dotyczące zachowania zwiększonej czujności.
    Podmiot przetwarzajacy zobowiązany jest do stosowania sie do wymogów ogłaszanych stopnii alarmowych (zagrożeń w cyberprzestrzeni), zgłaszania Administratorowi wszelkich informacji o anomaliach w pracy komputerów, w tym poczty e-mail pod nr tel. 94-34-88-460.

14. Wymagania dotyczące rozliczalności.
Podmiot przetwarzajacy na żądanie Administratora jest w stanie wykazać, że osoby, którym udzielił dostępu do danych podlegają wyżej wymienionemu obowiązkowi zachowania poufności.

C.3 Pomoc dla Administratora.

1. Podmiot przetwarzajacy pomaga Administratorowi w wywiązywaniu się z obowiazków okreslonych w ust.11 Umowy.

2. Procedura postępowania w przypadku incydentu bezpieczeństwa, w tym naruszenia ochrony danych:

Podmiot przetwarzajacy zgłasza incydent bezpieczeństwa/naruszenie ochrony danych Administratorowi niezwłocznie po powzięciu wiadomości.

1) Zgłoszenie powinno nastąpić:

a) bez zbędnej zwłoki i w miarę możliwości, nie później niż w ciągu 8 godzin od powzięcia wiadomości, w sytuacji, gdy naruszenie będzie się wiązało się z zagrożeniem dla praw i wolności osób fizycznych,

b) bez zbędnej zwłoki i w miarę możliwości, nie później niż w ciągu 8 godzin od powzięcia informacjii, w sytuacji gdy incydent będzie się wiązał z przerwaniem ciagłości udzielania świadczeń opieki zdrowotnej lub obrotu i dystrybucji produktów leczniczych przez Administratora, jako operatora usługi kluczowej w sektorze ochrony zdrowia,

c) za pośrednictwem telefonu: 94 34 88 545 lub 94 34 88 151, korespondencji e-mail: sekretariat@swk.med.pl , ePUAP: swkoszalin

2) Zgłoszenie powinno zawierać co najmniej:

a) opis charakteru naruszenia (w tym, w miarę możliwości, kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz wpisów danych, których dotyczy naruszenie,

b) wskazanie prawdopodobnych konsekwencji naruszenia dla osób, których dane dotyczą

c) wskazanie środków, które Podmiot przetwarzający podjął lub zamierza podjąć w celu zaradzenia naruszeniu, w tym w celu zminimalizowania jego ewentualnych negatywnych skutków.

3) Jeżeli przekazanie wszystkich tych informacji równocześnie nie jest możliwe, Podmiot przekazuje w zgłoszeniu informacje dostępne w danej chwili, a po uzyskaniu dostępu do dalszych informacji przekazuje się je bez zbędnej zwłoki.

C.4 Okres przechowywania / procedury usuwania

	Okres przechowywania / procedury usuwania	
1.	Dane osobowe są przechowywane w systemie informatycznym, po czym są automatycznie usuwane przez Podmiot przetwarzający.	Nie dotyczy
2.	Po zakończeniu świadczenia usług Podmiot przetwarzający usuwa lub zwraca dane osobowe, w zależności od wyboru administratora.	Nie dotyczy
3.	Dane osobowe pacjentów zarejestrowane na nośnikach papierowych i elektronicznych stanowią dokumentację medyczną, przechowywaną zgodnie z przepisami.	

C.5 Miejsce przetwarzania

Przetwarzanie danych osobowych objętych Umową nie może, bez uprzedniej pisemnej zgody Administratora danych, odbywać się w miejscach innych niż:

a) siedziba Szpitala, ul. T. Chałubińskiego 7 w Koszalinie
b) miejsce zamieszkania lub pobytu świadczeniobiorcy.

C.6 Instrukcje dotyczące przekazywania danych osobowych do państw trzecich

Umowa nie przewiduje transferu danych do Państw Trzecich.

C.7 Procedury audytów, w tym kontroli przetwarzania danych osobowych.

I Audyt/ kontrola Podmiotu przetwarzajacego przeprowadzana przez stronę trzecią.

Strony nie przewidują prowadzenia audytów/ kontroli przez niezależną stronę trzecią.

II Audyt / kontrola Podmiotu przetwarzającego przeprowdzana przez Administratora.

1) Administrator danych lub przedstawiciel administratora danych ma prawo do:
   a) wglądu, w tym kontroli pomieszczeń, w których Podmiot przetwarzający przetwarza dane osobowe, w tym do systemów informatycznych wykorzystywanych i związanych z przetwarzaniem. Kontrole takie mogą być przeprowadzane, gdy Administrator uzna to za konieczne."

lub

   b) Administrator lub przedstawiciel Administratora przeprowadza okresową kontrolę polegającą na żadaniu udzielania pisemnej informacji lub wyjaśnień dotyczących wykorzystywanych sposobów oraz środków zabezpieczających dane, w celu ustalenia, czy Podmiot przetwarzający spełnia obowiązujące przepisy dotyczące ochrony danych osobowych.
2) Oprócz planowej kontroli Administrator danych może przeprowadzić fizyczną kontrolę miejsc, w których przetwarzane są dane osobowe, gdy administrator danych uzna to za konieczne, w szczególności w sytuacji wystąpienia incydentu bezpieczeństwa w tym naruszenia ochrony danych.
3) Administrator powiadomi Podmiot przetwarzajacy o zamiarze przeprowadzenia audytu/kontroli, w terminie wspólnie ustalonym przez Strony, nie później jednak niż 3 dni robocze od dnia powiadomienia o zamiarze przeprowadzenia audytu/kontroli.
4) W przypadku powzięcia przez Administratora informacji o rażącym naruszeniu zobowiązań wynikających z niniejszej Umowy/przepisów ustawy o ochronie danych osobowych/ rozporzadzenia o ochronie danych/ wymagań prawnych lub wystapienia incydentu bezpieczeństwa, w tym naruszenia ochrony danych Administratorowi przysługuje uprawnienie do dokonania niezapowiedzianej kontroli.
5) Ponadto Podmiot przetwarzajacy zobowiązuje się do udostępnienia organom nadzorczym, lub przedstawicielom działającym w imieniu tych organów nadzorczych, dostępu do pomieszczeń Podmiotu przetwarzającego, za okazaniem odpowiednich uprawnień.

6) Podmiot przetwarzajacy jest zobowiązany do zastosowania się do zaleceń pokontrolnych sformułowanych przez Administratora dotyczących zabezpieczenia danych osobowych/ informacji.
7) Podmiotowi przetwarzajacemu przysługuje prawo:
   a) kierowania zapytań do Administratora w zakresie prawidłowości wykonania obowiązków dotyczących zabezpieczania powierzonych danych osobowych/informacji chronionych,
   b) do odmowy udzielenia pisemnej informacji lub wyjaśnień oraz udzielenia dostępu do miejsc przetwarzania danych osobowych, prawo ograniczenia wglądu do dokumentów, jeśli informacje, dokumenty lub ich części zawierają tajemnicę przedsiębiorstwa lub ich ujawnienie groziłoby ujawnieniem innych tajemnic podlegających ochronie na podstawie odrębnych przepisów.
8) Administrator może zdecydować o rozpoczęciu i udziale w audycie/ kontroli Podwykonawcy, w przypadku, gdy nadzór Podmiotu przetwarzającego nad Podwykonawcą nie dał Administratorowi wystarczającej pewności, że przetwarzanie przez Podwykonawcę odbywa się zgodnie z Umową, rozporządzeniem o ochronie danych osobowych, przepisami prawa.
9) Zaaangażowanie Administratora w kontrolę Podwykonawcy nie zwalnia Podmiotu przetwarzajacego z odpowiedzialności za powierzone do przetwarzania dane.

Załącznik D. Pozostałe uzgodnienia Stron.

Nr Załącznika	Wersja	Nr Umowy Głównej	Wprowadzone zmiany	Czas trwania powierzenia przetwarzania	Data aktualizacji
D.	0.1		określone w pkt.od D1do D5		
	1.0				

D1. Procedura nadawania uprawnień do systemu informatycznego ESKULAP.

Podmiot przetwarzający prowadzi rejestr wniosków o nadanie, modyfikację uprawnień. Nadawanie uprawnień odbywa się wg poniższego schematu.

1. Podmiot przetwarzający, z wyprzedzeniem co najmniej 1 dnia, w godzinach od 7.25-14.00 przekazuje Administratorowi wypełniony wniosek o nadanie lub zmianę uprawnienia do systemu informatycznego ESKULAP. Załącznik nr D.1.1
2. Sposób przekazania wniosku zostanie indywidualnie uzgodniony przez Strony.
3. Pracownik Działu Informatyki nadaje uprawnienia do sytemu informatycznego Eskulap.
4. Hasło i login zostanie indywidualnie przekazane pracownikowi wskazanemu we wniosku.

D.2 Procedura odbierania uprawnień do systemu informatycznego ESKULAP.

1. Podmiot przetwarzający informuje Administratora, na co najmniej 2 dni przed upływem uprawnień, o odebraniu pracownikowi uprawnień do systemu informatycznego ESKULAP.
2. Pracownik Działu Informatyki unieważnia hasło dostępu i wyrejestrowuje identyfikator z systemu informatycznego.
3. Nie wypełnienie przez Podmiot przetwarzający obowiązku poinformowania Administratora o odebraniu uprawnienia do obsługi systemu informatycznego ESKULAP skutkować będzie zapłatą kar umownych w wysokości 10% wynagrodzenia za swiadczone usługi.

D.3 Wzór wniosku o nadanie/ modyfikację uprawnień do systemu informatycznego Eskulap**.**

.....
Podmiot przetwarzający
Miejscowość, data

Imię i nazwisko pracownika.....

Stanowisko.....

WNIOSEK O NADANIE/ MODYFIKACJĘ UPRAWNIEŃ DO SYSTEMU INFORMATYCZNEGO ESKULAP

Rodzaj zgłoszenia:

1. Nadanie uprawnień od dnia……..
data
2. Zmiana uprawnień (*rozszerzenie, zmniejszenie zakresu uprawnień*) od dnia …….....

3. Odebranie uprawnień od dnia

Podmiot Przetwarzający Administrator

.....
Data i podpis Inspektora Ochrony Danych

.....
Data i podpis Kierownika Działu Informatyki

D.4 Zasady udostępniania nagrań rozmów telefonicznych. Wyciąg z Regulaminu nagrywania rozmów telefonicznych, Zarządzenie Nr 31.2019 Dyrektora Szpitala Wojewódzkiego im. M. Kopernika w Koszalinie z dnia 13.02.2019.

1. Rozmowy telefoniczne rejestrowane są na wbudowanym w centrali telefonicznej nośniku danych. Centrala telefoniczna znajduje się w budynku administracyjnym Szpitala Wojewódzkiego im. M. Kopernika, przy ul. Chałubińskiego 7 w Koszalinie.
2. Udostępnianie rozmowy telefonicznej (przesłuchanie nagrania lub kopiowanie na zewnętrzny nośnik) odbywa się wyłącznie za zgodą Dyrektora, na wniosek:
    a) osoby, której dane dotyczą,
    b) organów państwowych, organów ochrony prawnej (Policji, Prokuratury, Sądu) lub organów samorządu terytorialnego, w związku z prowadzonym postępowaniem i na podstawie odpowiednich przepisów prawa.
    3. nagrywanie rozmów telefonicznych na zewnętrzny nośnik danych, odbywa się w przypadku, gdy nagrania stanowią dowód w postępowaniu lub na zasadach określonych w § 6 ust. 3 pkt 3.

4.Zasady obowiązujące przy udostępnianiu nagrań rozmów telefonicznych:

    a) osoba uprawniona składa wniosek do Dyrektora Szpitala o udostępnienie nagrania.
    b) w przypadku wydania zgody, Inspektor ds. organizacyjnych uzgadnia z osobą wnioskującą termin przesłuchania nagrania, w przypadku odmowy udostępnienia nagrania zawiadamia o tym osobę wnioskującą,
    c) przesłuchanie nagrania lub utrwalenie nagrania na zewnętrznym nośniku informacji odbywa się w obecności Inspektora ds. organizacyjnych upoważnionego do prowadzenia sprawy i wnioskodawcy,
    d) z wszystkich czynności podjętych podczas udostępniania nagrania, tj. przesłuchania nagrania lub utrwalenia na zewnętrznym nośniku informacji ww. pracownicy sporządzają Protokół przekazania.
    e) osoba uprawniona potwierdza udostępnienie nagrania w Protokole przekazania,
    f) opakowanie nośnika przeznaczonego do wysyłki Inspektor ds. organizacyjnych opatruje pieczęcią oraz podpisem,
    g) Inspektor ds. organizacyjnych prowadzi ewidencję wniosków o udostępnienie nagrania i archiwizuje Protokoły przekazania,

h) kopie nagrań są przechowywane na serwerze przez czas nie dłuższy, niż jest to niezbędne do osiągnięcia celu.

D. 5 Wzór wniosku o udostępnienie nagrania rozmowy telefonicznej

(Zakres niezbędnych informacji, które powinien przekazać wnioskodawca):

1. Adresat wniosku: Dyrektor Szpitala Wojewódzkiego im. M. Kopernika w Koszalinie, ul. T. Chałubińskiego 7, 75-581 Koszalin:

2. Wnioskodawca:

……...
(imię, nazwisko i dane do kontaktu)

3. Uzasadnienie wniosku:

……
(cel, zakres, podstawa prawna)

4. Dane niezbędne do identyfikacji nagrania:

……
(data i przybliżona godzina rozmowy telefonicznej, numer telefonu, którego dotyczy wniosek)

5. Sposób udostępnienia nagrania rozmowy telefonicznej:

……
(przesłuchanie nagrania, wykonanie kopii)

6. Sposób rozpatrzenia wniosku:

.....
(zgoda, odmowa)

…….....
(data, podpis oraz pieczęć wnioskodawcy)