POLITYKA OCHRONY DANYCH OSOBOWYCH

WOJEWÓDZKIEGO SZPITALA ZESPOLONEGO W ELBLĄGU

Stan na 15 października 2018 r.

Spis treści

1. **Wstęp**

1.1. Niniejsza Polityka ochrony danych osobowych jest dokumentem opisującym sposób przetwarzania danych osobowych oraz obowiązki Wojewódzkiego Szpitala Zespolonego w Elblągu działającego w charakterze Administratora danych osobowych (dalej Administrator danych), przetwarzanych w związku z prowadzoną działalnością leczniczą.

1.2. Niniejsza Polityka poddawana jest bieżącej aktualizacji, nie rzadziej niż raz do roku.

1.3. Słownik:

1) **administrator** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;

2) **dane osobowe (dane)** - informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

3) **dane dotyczące zdrowia** - dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej - w tym o korzystaniu z usług opieki zdrowotnej - ujawniające informacje o stanie jej zdrowia; do danych o stanie zdrowia należą także:
   a) informacje o danej osobie fizycznej zbierane podczas jej rejestracji do usług opieki zdrowotnej lub podczas świadczenia jej usług opieki zdrowotnej, takie jak w szczególności: numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby fizycznej do celów zdrowotnych;
   b) informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych;
   c) wszelkie informacje, na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym lub biomedycznym osoby, której dane dotyczą, niezależnie od ich źródła, którym może być na przykład lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne in vitro;

4) **zbiór danych** - uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

5) **Inspektor Ochrony Danych (IOD)** - inspektor w rozumieniu art. 37 Rozporządzenia;

6) **Administrator Bezpieczeństwa Systemów Informatycznych (ABSI)** - osoba powołana przez Administratora danych, odpowiedzialna za kontrolę nad właściwym poziomem stosowania zabezpieczeń serwerów, sieci, oprogramowania i sprzętu

informatycznego w sposób zapewniający właściwy poziom ochrony poufności, integralności i dostępności informacji zawartych w systemach informatycznych ze szczególnym uwzględnieniem ochrony danych osobowych;

7) **Lokalny Administrator Systemów Informatycznych (LAIT)** - pracownik Sekcji Informatycznej i Telekomunikacji, któremu w Karcie zadań, uprawnień i obowiązków powierzono min. zarządzanie kontami i uprawnieniami użytkowników, przeglądy, konserwację systemów informatycznych i elektronicznych nośników informacji oraz zabezpieczenie systemów informatycznych przed szkodliwym oprogramowaniem;

8) **Lokalny Administrator Zbiorów Danych Osobowych (LAZDO) -** kierownik, osoba kierująca zespołem pracowników Szpitala w rozumieniu Regulaminu Organizacyjnego Wojewódzkiego Szpitala Zespolonego w Elblągu;

9) **odbiorca** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią; nie są odbiorcami organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego;

10) **podmiot przetwarzający** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

11) **przetwarzanie** - operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taki jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

12) **system informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;

13) **użytkownik** - osoba upoważniona do przetwarzania danych osobowych w wersji papierowej oraz w systemie informatycznym, posiadająca ustalony identyfikator, hasło i uprawnienia do dostępu do danych osobowych gromadzonych w systemach informatycznych;

14) **identyfikator użytkownika** - ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

15) **hasło użytkownika** - ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawionej do pracy w systemie informatycznym;

16) **naruszenie ochrony danych osobowych** - naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania,

nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

17) **naruszenie zabezpieczenia systemu informatycznego** - jakiekolwiek naruszenie poufności, integralności, dostępności, autentyczności, niezawodności i bezpieczeństwa systemu informatycznego powstałe samoistnie w systemie, bądź dokonane przez osoby nieuprawnione lub uprawnione, działające w złej wierze albo omyłkowo;

18) **Rozporządzenie (RODO)** - Rozporządzenie 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;

19) **Urząd Ochrony Danych Osobowych (UODO)** - organ publiczny powołany w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych;

20) **Szpital** - Wojewódzki Szpital Zespolony w Elblągu.

1.4. Wojewódzki Szpital Zespolony w Elblągu jako Administrator danych stosuje zatwierdzony przez Urząd Ochrony Danych Osobowych kodeks postępowania dla sektora ochrony zdrowia.

2. Cele Polityki ochrony danych osobowych

2.1. Celem Polityki ochrony danych osobowych jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania w Szpitalu informacji zawierających dane osobowe. Ochrona danych osobowych realizowana jest poprzez odpowiednie zabezpieczenie organizacyjne i techniczne, w tym oprogramowanie systemowe oraz aplikacje.

2.2. Cele osiągane są przez:

1) prawidłowe zarządzanie obiegiem i przetwarzaniem danych osobowych;
2) właściwą ochronę danych osobowych, w szczególności danych szczególnie chronionych;
3) zarządzanie ryzykiem w celu ograniczenia go do akceptowanego poziomu;
4) cykliczne szkolenie osób upoważnionych do przetwarzania danych osobowych;
5) podnoszenie świadomości personelu w zakresie ochrony danych osobowych.

3. Zasady przetwarzania danych osobowych

3.1. Administrator danych przetwarza dane osobowe z poszanowaniem poniższych zasad:

1) **zasada legalności, rzetelności i przejrzystości** – dane powinny być przetwarzane zgodnie z prawem, rzetelnie poprzez dbałość o aktualność danych oraz ich poprawność i w sposób przejrzysty dla osoby, której dane dotyczą;

2) **zasada ograniczenia celu** - dane powinny być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych, historycznych lub statystycznych nie jest uznawane za niezgodne z pierwotnymi celami;

3) **zasada minimalizacji danych (zasada adekwatności)** - dane powinny być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;

4) **zasada ograniczenia przechowywania** - dane musza być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w jakich dane osobowe zostały pozyskane;

5) **zasada zapewnienia bezpieczeństwa danych, w tym ich integralności i poufności** - dane muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych i organizacyjnych.

3.2. Administrator danych zapewnia rozliczalność - jest w stanie wykazać przestrzeganie wszystkich zasad, o których mowa w pkt 3.1, w szczególności poprzez wdrożenie środków(w tym wewnętrznych procedur) gwarantujących przestrzeganie przepisów o ochronie danych osobowych w związku z operacjami ich przetwarzania, jak również poprzez sporządzenie dokumentacji wskazującej osobom, których dane dotyczą, organom nadzorczym, a także innym interesariuszom, jakie środki podjęto, aby zapewnić przestrzeganie tych przepisów.

4. Podstawy prawne przetwarzania danych osobowych

4.1. Działalność Administratora danych jako podmiotu leczniczego regulują w szczególności:

1) ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta;
2) ustawa o działalności leczniczej;
3) ustawa o służbie medycyny pracy;
4) ustawa o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi;
5) ustawa o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych;
6) ustawa o zawodach lekarza i lekarza dentysty;
7) rozporządzenie Ministra Zdrowia w sprawie szczegółowych wymagań, jakim powinny odpowiadać pomieszczenia i urządzenia podmiotu wykonującego działalność leczniczą;
8) rozporządzenie Ministra Zdrowia w sprawie rodzajów dokumentacji medycznej służby medycyny pracy, sposobu jej prowadzenia i przechowywania oraz wzoru stosowanych dokumentów;
9) rozporządzenie Ministra Zdrowia w sprawie rodzajów i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania.

4.2. Jako podmiot leczniczy, Administrator danych przetwarza dane osobowe w celach zdrowotnych na podstawie art. 9 ust. 2 lit. h Rozporządzenia.

4.3. Przez cele zdrowotne rozumie się:

1) **profilaktykę zdrowotną** - w szczególności poprzez informowanie pacjentów o możliwości pobierania świadczeń zdrowotnych, przekazywanie materiałów edukacyjnych;
2) **medycynę pracy oraz ocenę zdolności pracownika do pracy** - w szczególności poprzez sprawowanie zadań jednostki służby medycyny pracy, w tym poprzez badania wstępne, okresowe oraz kontrolne na podstawie umowy zawartej pomiędzy administratorem a pracodawcą;
3) **diagnozę medyczną oraz leczenie** - w szczególności poprzez udzielanie świadczeń zdrowotnych oraz prowadzenie dokumentacji medycznej;
4) z**apewnienie opieki zdrowotnej oraz zarządzanie systemami opieki zdrowotnej** - w szczególności poprzez rejestrację pacjenta do usług administratora, odbieranie oraz archiwizację oświadczeń pacjentów wynikających z realizacji ich praw pacjenta, wykorzystywanie i utrzymywanie infrastruktury informatycznej służącej wspieraniu

procesu leczenia, rozliczanie udzielonych świadczeń, wymianę danych osobowych pacjenta z innym podmiotem leczniczym w ramach zachowania ciągłości leczenia.

4.4. W zakresie wykraczającym poza cele zdrowotne Administrator danych` przetwarza dane na podstawie:

1) zgody pacjenta (art. 6 ust. 1 lit. a Rozporządzenia) - w celach marketingowych;

2) prawnie uzasadnionego interesu administratora (art. 6 ust. 1 lit. f Rozporządzenia) - w celu dochodzenia roszczeń i obrony przed roszczeniami.

4.5. Zgoda, o której mowa w pkt 4.4.1. jest dobrowolna i jej wyrażenie jest świadomym działaniem pacjenta. Nieudzielenie zgody nie powoduje dla pacjenta żadnych negatywnych konsekwencji, w szczególności nie skutkuje odmową udzielenia świadczenia zdrowotnego ani nie warunkuje udzielenia tego świadczenia.

5. Obowiązki Administratora danych

Środki techniczne i organizacyjne

5.1. Administrator danych stosuje środki organizacyjne oraz techniczne w celu zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzanych danych osobowych, z uwzględnieniem stanu wiedzy technicznej, kosztu wdrożenia, charakteru, zakresu, kontekstu i celu przetwarzania, ryzyka naruszenia praw lub wolności o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia. Stosowane środki techniczne i organizacyjne służą zapewnieniu poufności, integralności oraz rozliczalności przetwarzanych danych osobowych wymaganych przez Rozporządzenie(RODO).

5.2. Administrator Danych wdraża w szczególności następujące środki organizacyjne:

1) niniejszą Politykę, która określa zasady ochrony danych osobowych w Szpitalu, Instrukcję - Zarządzanie Systemem informatycznym w zakresie ochrony danych osobowych oraz Instrukcję - Postępowanie w przypadku naruszenia ochrony danych osobowych;

2) system upoważnień do przetwarzania danych osobowych w celu ograniczenia ilości pracowników Szpitala mających dostęp do konkretnych danych osobowych. W tym celu Administrator danych prowadzi rejestr osób upoważnionych oraz przechowuje treść zobowiązań do zachowania poufności. Wzory zobowiązania do zachowania poufności, wniosku o nadanie/modyfikację/odebranie uprawnień, upoważnienia do

przetwarzania danych osobowych, rejestru osób upoważnionych do przetwarzania danych osobowych, odpowiednio: Nr 4, Nr 6, Nr 7 i Nr 11 do niniejszej Polityki;

3) umowy powierzenia przetwarzania danych osobowych- wzór umowy stanowi Załącznik Nr 12 do Polityki

4) klauzule informacyjne, w tym Informacja na temat przetwarzania danych osobowych pacjentów przez Wojewódzki Szpital Zespolony w Elblągu która stanowi Załącznik Nr 17 do Polityki.

5) system uprawnień dostępowych do systemów informatycznych w celu ograniczenia ilości administratorów systemów informatycznych mających dostęp do konkretnych systemów;

6) wyznaczenie Inspektora Ochrony Danych i Administratora Bezpieczeństwa Systemów Informatycznych;

7) wstępne i okresowe szkolenia pracowników z zasad ochrony danych osobowych;

8) wykonywanie zadań sprawdzających przestrzeganie zasad ochrony danych osobowych na komórkach organizacyjnych i stanowiskach pracy

9) środki zapewniające szybkie przywrócenie dostępności danych osobowych i dostęp do nich w razie incydentu fizycznego lub technicznego;

10) regularne testowanie, mierzenie i ocenę skuteczności tych środków.

5.3. Środki techniczne wdrażane przez Administratora danych to w szczególności:

1) fizyczna ochrona pomieszczeń – zatrudnienie firmy ochroniarskiej;

2) bariery fizyczne w dostępie do pomieszczeń – zamykanie drzwi i szaf na klucz;

3) fizyczna ochrona serwerowni – klimatyzacja, system przeciwpożarowy, awaryjne zasilanie, zapasowe łącze internetowe;

4) monitoring wizyjny na terenie Szpitala;

5) cyklicznie sporządzane kopie zapasowe kluczowych systemów IT.

5.4. Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych osobowych oraz sposób ich zabezpieczenia, w szczególności w postaci procedur, wytycznych oraz formularzy.

5.5. Administrator danych opracowuje i wdraża procedury gwarantujące ochronę prywatności na etapie powstawania nowych projektów, inwestycji oraz zmian wprowadzonych przez administratora w procesach z udziałem danych osobowych.

Rejestr czynności przetwarzania danych osobowych i rejestr kategorii czynności przetwarzania danych osobowych.

5.6. Administrator danych prowadzi rejestr czynności przetwarzania danych osobowych oraz rejestr kategorii czynności przetwarzania danych osobowych. Rejestry te są prowadzone w formie pisemnej i elektronicznej.

5.7. Rejestr kategorii czynności przetwarzania jest prowadzony przez Szpital dla umów powierzenia przetwarzania danych osobowych, w których występuje on w charakterze podmiotu przetwarzającego(procesora).

5.8. Rejestr czynności przetwarzania danych osobowych zawiera:

1) imię i nazwisko/ nazwę oraz dane kontaktowe Administratora danych oraz Inspektora Ochrony Danych;
2) nazwę zbioru;
3) czynność przetwarzania danych osobowych;
4) komórkę organizacyjną/stanowisko;
5) określenie celu przetwarzania;
6) formę przetwarzania - nazwę systemu lub oprogramowania;
7) podstawę prawną przetwarzania;
8) opis kategorii osób, których dane dotyczą;
9) kategorie danych osobowych przetwarzanych w ramach zbioru;
10) nazwę podmiotu przetwarzającego i dane kontaktowe;
11) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione (innych niż podmiot przetwarzający);
12) operacje przetwarzania wykonywane na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowny;
13) planowany termin usunięcia/zniszczenia danych osobowych;
14) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa;
15) planowane terminy usunięcia poszczególnych kategorii danych (jeżeli możliwe jest ich wskazanie);
16) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa;
17) ocenę ryzyka;
18) ocenę skutków dla ochrony danych osobowych;
19) zapis o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej.

5.9. Rejestr kategorii czynności przetwarzania dokonywanych w imieniu administratora zawiera:

1) imię i nazwisko/ nazwę oraz dane kontaktowe podmiotu przetwarzającego oraz inspektora ochrony danych;

2) imię i nazwisko/nazwę każdego administratora, w imieniu którego działa podmiot przetwarzający oraz inspektora ochrony danych (jeśli wyznaczono);
3) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
4) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe);
5) informację o umowie powierzenia (numer, data czas trwania);
6) opis kategorii osób, których dane dotyczą;
7) cel przetwarzania danych;
8) formę przetwarzania- nazwę systemu lub oprogramowania;
9) podstawę prawną przetwarzania;
10) kategorie danych osobowych (zwykłe / szczególnej kategorii);
11) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione;
12) czas trwania przetwarzania;
13) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe);
14) nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane;
15) dokumentację odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust. 1 akapit drugi RODO;

5.10. Rejestr czynności przetwarzania i rejestr kategorii czynności przetwarzania są na bieżąco aktualizowane i udostępniane na żądanie UODO.

5.11. W imieniu Administratora danych/podmiotu przetwarzającego rejestr czynności przetwarzania i rejestr kategorii czynności przetwarzania prowadzi Inspektor Ochrony Danych. Rejestry stanowią odpowiednio Załączniki Nr 14 i Nr 15 do niniejszej Polityki.

Inspektor ochrony danych

5.12. Administrator danych jako samodzielny publiczny zakład opieki zdrowotnej wyznacza Inspektora Ochrony Danych (IOD) i dokonuje zawiadomienia o wyznaczeniu Inspektora do Urzędu Ochrony Danych Osobowych.

5.13. Wyznaczenie IOD następuje na podstawie jego kwalifikacji zawodowych, w tym wiedzy oraz zdobytego doświadczenia, które to kwalifikacje zostały udokumentowane.

5.14. Administrator danych stwarza IOD odpowiednie warunki, aby mógł realizować swoje obowiązki, w szczególności poprzez:

1) niezwłoczne oraz odpowiednie włączanie go we wszystkie sprawy dotyczące ochrony danych osobowych w Szpitalu;

2) zapewnienie zasobów niezbędnych do wykonywania jego zadań oraz utrzymania jego fachowej wiedzy;

3) zapewnienie mu niezależności w sprawowaniu jego funkcji, m.in. poprzez niewydawanie instrukcji dotyczących wykonywania przez niego jego zadań, nieponoszenie przez IOD negatywnych konsekwencji za wypełnianie przez niego jego zadań, zapewnienie odpowiedniej struktury organizacyjnej, aby podlegał jedynie najwyższemu kierownictwu Szpitala.

5.15. Zadania IOD obejmują w szczególności:

1) podnoszenie świadomości wśród personelu przetwarzającego dane osobowe oraz podmiotów przetwarzających dane osobowe na zlecenie Administratora danych, poprzez realizację szkoleń oraz informowanie o obowiązkach spoczywających na tych osobach i podmiotach;

2) monitorowanie przestrzegania przez Administratora danych przepisów Rozporządzenia i innych przepisów prawa ochrony danych osobowych oraz regulacji wewnętrznych przyjętych u Administratora danych regulujących kwestie związane z przetwarzaniem danych osobowych;

3) wykonywanie audytów w kwestiach związanych z przetwarzaniem danych osobowych;

4) uczestniczenie oraz wspieranie Administratora danych w dokonywaniu oceny skutków dla ochrony danych oraz monitorowanie wykonania oceny tych skutków;

5) współpraca z Urzędem Ochrony Danych Osobowych;

6) sprawowanie funkcji punktu kontaktowego dla pacjentów w kwestiach związanych z przetwarzaniem danych osobowych.

6. Prawa osób, których dane dotyczą

6.1. Administrator danych:

1) przetwarza dane osobowe z poszanowaniem praw pacjenta oraz praw osób, których dane dotyczą wynikających z Rozporządzenia;

2) prowadzi rejestr zgłoszonych żądań przez osoby, których danych dotyczą - Załącznik Nr 17 do Polityki;

3) przed wykonaniem praw osoby, której dane dotyczą dokonuje weryfikacji tożsamości osoby zgłaszającej żądanie, celem ustalenia, czy żądanie pochodzi od osoby uprawnionej;

4) zapewnia odpowiednie zaplecze techniczne oraz kadrowe w celu terminowej oraz rzetelnej realizacji praw osoby, której dane dotyczą. Zgłoszone żądania realizowane są przez administratora niezwłocznie, nie później niż w terminie miesiąca od otrzymania żądania. W przypadku niemożności wykonania żądania w w/w terminie, z uwagi na skomplikowany charakter sprawy, administrator kontaktuje się z pacjentem i informuje go o przyczynie wydłużenia tego terminu oraz przewidywanym terminie realizacji żądania pacjenta.

Prawo do informacji

6.2. Pacjenci są informowani przez Administratora danych o sposobie przetwarzania ich danych osobowych oraz przysługującym ich uprawnieniach w formie klauzuli informacyjnej, z którą mogą zapoznać się w każdej chwili w jego siedzibie, w każdej medycznej komórce organizacyjnej, w tym w Izbie Przyjęć oraz na stronie internetowej Szpitala. Informacja na temat przetwarzania danych osobowych pacjentów przez Wojewódzki Szpital Zespolony w Elblągu stanowi Załącznik Nr 18 do Polityki.

6.3. Klauzula informacyjna jest sporządzona prostym językiem, w sposób przejrzysty i wyczerpuje wszystkie informacje zgodnie z art. 13 oraz 14 Rozporządzenia.

Prawo dostępu do danych

6.4. Na żądanie pacjenta Administrator danych udziela mu informacji o sposobie przetwarzania jego danych osobowych. Na żądanie pacjenta udostępnia mu nieodpłatnie pierwszą kopię jego danych osobowych. Za każdą kolejną kopię Administrator danych może pobrać opłatę w rozsądnej wysokości (w tym za wydanie kopii w formie papierowej pobierana jest opłata zgodnie z przepisami regulującymi stawki za każdą wydaną stronę dokumentacji medycznej).

6.5. Jeżeli żądanie wydania kopii danych zostało złożone w formie elektronicznej a pacjent nie zaznaczył inaczej - kopia wydawana jest w tej samej formie.

6.6. Administrator danych może udostępnić kopię w inny sposób, niż wybrany przez pacjenta, jeżeli ze względów technicznych nie jest to możliwe (np. ze względu na wagę pliku w wersji elektronicznej); o niemożności dostarczenia kopii w wybrany przez

pacjenta sposób oraz proponowanym alternatywnym rozwiązaniu Administrator danych niezwłocznie powiadamia pacjenta.

Prawo do sprostowania danych

6.7. Administrator danych umożliwia pacjentowi niezwłoczne sprostowanie jego danych osobowych, jeżeli są one nieprawidłowe lub nieaktualne, lub ich uzupełnienie.

6.8. Administrator danych może żądać od pacjenta stosownych dokumentów w celu okazania, aby ustalić zasadność oraz zgodność z prawem dokonywanej zmiany danych osobowych.

Prawo do usunięcia danych (prawo do bycia zapomnianym)

6.9. Administrator danych usuwa bez zbędnej zwłoki dane osobowe pacjenta na żądanie pacjenta, jeżeli na administratorze nie spoczywają obowiązki nakazujące dalsze przetwarzanie danych osobowych.

6.10. Administrator danych odmawia realizacji prawa do bycia zapomnianym, jeżeli została wytworzona dokumentacja medyczna pacjenta i nie upłynął okres jej przechowywania wynikający z przepisów regulujących sposób oraz okres prowadzenia oraz przechowywania dokumentacji medycznej.

6.11. Odmowa realizacji prawa do usunięcia danych jest przekazywana przez Administratora danych pacjentowi wraz z uzasadnieniem przyczyny odmowy zawierającym podstawy prawne odmowy.

Prawo do ograniczenia przetwarzania

6.12. Z uwagi na fakt, iż realizacja prawa do ograniczenia przetwarzania danych znacznie utrudniłaby realizację celów zdrowotnych, o których mowa w pkt 3.3., pomimo zgłoszonego żądania ograniczenia przetwarzania danych, Administrator danych jest uprawniony do ich przetwarzania w dalszym zakresie (w szczególności zawartych w dokumentacji medycznej lub innych danych, przetwarzanych w oparciu o art. 9 ust. 2 lit. h Rozporządzenia.

Prawo do przenoszenia danych

6.13. Dla danych osobowych przetwarzanych w oparciu o podstawę prawną - art. 9 ust. 2 lit. h, Rozporządzenia wobec administratora będącego podmiotem leczniczym, prawo do przenoszenia danych nie znajduje zastosowania.

6.14. W sytuacji odmowy realizacji żądania prawa do przenoszenia danych, administrator informuje pacjenta o przyczynie odmowy i instruuje pacjenta, jakie kroki może podjąć w celu przekazania dokumentacji medycznej do innego podmiotu leczniczego.

Prawo do sprzeciwu

6.15. Dla danych osobowych przetwarzanych przez administratora będącego podmiotem leczniczym, w oparciu o podstawę prawną - art. 9 ust. 2 lit. h Rozporządzenia, prawo do sprzeciwu nie znajduje zastosowania.

7. Naruszenia ochrony danych osobowych

7.1. Administrator danych opracował i wdrożył procedury postępowania w przypadku naruszeń lub podejrzeń naruszeń ochrony danych osobowych.

7.2. Administrator danych prowadzi rejestr naruszeń ochrony danych osobowych oraz dokumentuje wszystkie okoliczności związane z naruszeniami. Rejestr naruszeń ochrony danych osobowych stanowi Załącznik Nr 16.

7.3. W przypadku naruszeń ochrony danych osobowych mogących skutkować naruszeniem praw lub wolności pacjenta, Administrator danych dokonuje zgłoszenia takiego naruszenia Urzędowi Ochrony Danych Osobowych w terminie 72 godzin od stwierdzenia naruszenia.

7.4. W celu dotrzymania terminu, o którym mowa w pkt 7.3. Administrator danych wprowadza do umowy powierzenia przetwarzania danych lub innego instrumentu regulującego kwestię powierzenia przetwarzania danych, odpowiednie postanowienia zobowiązujące podmiot przetwarzający do niezwłocznego zgłaszania administratorowi wszelkich naruszeń ochrony danych osobowych oraz udzielania wszelkich okoliczności dotyczących tych naruszeń.

7.5. W przypadku, jeżeli naruszenie skutkowałoby wysokim ryzykiem naruszenia praw i wolności pacjenta, Administrator danych bez zbędnej zwłoki zawiadamia również tego pacjenta i informuje go jasnym i prostym językiem o okolicznościach naruszenia oraz podjętych środkach mających na celu zapobieżenie jego negatywnym skutkom.

8. Udostępnianie danych osobowych

8.1. Administrator danych udostępnia dane osobowe podmiotom trzecim zgodnie z przepisami ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta. W szczególności udostępnia dane osobowe pacjenta osobom upoważnionym przez pacjenta.

8.2. Przed udostępnieniem danych osobowych pacjenta Administrator danych podejmuje niezbędne czynności mające na celu ustalenie tożsamości pacjenta, osoby upoważnionej oraz zakresu upoważnienia.

9. **Znaczenie** P**olityki ochrony danych osobowych dla Wojewódzkiego Szpitala Zespolonego w Elblągu**

9.1. Realizowanie misji, celów oraz zadań Szpitala w obszarach polityki zdrowotnej jest silnie uzależnione od:

1) sprawnego obiegu i przetwarzania informacji skorelowanej ze strukturą organizacyjną, podejmowanych decyzji opartych o informacje aktualne, rzetelne, dokładne, zrozumiałe, kompletne, łatwe i szybko dostępne;
2) skutecznej ochrony i bezpieczeństwa udostępniania oraz przechowywania tych informacji bez względu na wykorzystywane nośniki ich przekazywania.

9.2. Politykę ochrony danych osobowych stosuje się do przetwarzania danych osobowych:

1) w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych zgromadzonych w jednej lub rozproszonych funkcjonalnie w wielu komórkach organizacyjnych Szpitala;
2) w systemach informatycznych;
3) sporządzanych doraźnie, wyłącznie ze względów technicznych, szkoleniowych, a po ich wykorzystaniu niezwłocznie usuwanych, albo poddawanych anonimizacji.

10.Struktura dokumentacji w zakresie Polityki bezpieczeństwa danych osobowych

10.1.W skład Polityki bezpieczeństwa danych osobowych wchodzą następujące dokumenty:

1) Polityka ochrony danych z następującymi załącznikami:

a) Wykaz budynków i pomieszczeń, w których przetwarzane są dane osobowe - Załącznik Nr 1;
b) Wykaz zbiorów danych osobowych -Załącznik Nr 2;
c) Instrukcja „System monitoringu wizyjnego Wojewódzkiego Szpitala Zespolonego w Elblągu”- Załącznik Nr 3;
d) Wzór zobowiązania do zachowania poufności – pracownicy zatrudnieni na podstawie umowy o pracę /kontraktu cywilnoprawnego- Załącznik Nr 4;
e) Wzór zobowiązania do zachowania poufności – studenci, praktykanci - Załącznik Nr 5;
f) Wzór wniosku o nadanie/ modyfikację/odebranie uprawnień do przetwarzania danych osobowych - Załącznik Nr 6;
g) Wzór upoważnienia do przetwarzania danych osobowych – pracownicy zatrudnieni na podstawie umowy o pracę/ kontraktu cywilnoprawnego -Załącznik Nr 7;
h) Wzór modyfikacji upoważnienia do przetwarzania danych osobowych - Załącznik Nr 8;
i) Wzór odebrania upoważnienia do przetwarzania danych osobowych - Załącznik Nr 9;
j) Karta szkolenia wstępnego z zakresu ochrony danych osobowych - Załącznik Nr 10;
k) Rejestr osób upoważnionych do przetwarzania danych osobowych- Załącznik Nr 11;
l) Wzór umowy powierzenia przetwarzania danych osobowych- Załącznik Nr 12;
m) Rejestr umów powierzenia przetwarzania danych osobowych - Załącznik Nr 13;
n) Rejestr czynności przetwarzania danych osobowych- Załącznik Nr 14;
o) Rejestr kategorii czynności przetwarzania danych osobowych- Załącznik Nr 15;
p) Rejestr naruszeń ochrony danych osobowych – Załącznik nr 16;
q) Rejestr zgłoszonych żądań przez osoby, których dane dotyczą – Załącznik Nr 17.
r) Informacja na temat przetwarzania danych osobowych pacjentów przez WSZ w Elblągu – Załącznik Nr 18;

2**)** Instrukcja „Zarządzanie systemem informatycznym w zakresie ochrony danych osobowych”- Iadm-02-01;

3) Instrukcja „Postępowanie w przypadku naruszenia ochrony danych osobowych” - Iadm-2-02

10. 2. Upoważnienie do przetwarzania danych osobowych

10.2.1. Dostęp do przetwarzania danych osobowych mogą mieć wyłącznie osoby posiadające imienne upoważnienie do przetwarzania danych osobowych wydane przez Administratora

danych z wyłączeniem osób wykonujących zawód medyczny zobowiązanych do zachowania tajemnicy zawodowej (np. lekarze, pielęgniarki, ratownicy medyczni), którzy są upoważnieni do przetwarzania danych osobowych pacjentów z mocy ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta.

10.2.2. Każdy nowo zatrudniony pracownik/ osoba, z którą zawarto kontrakt cywilnoprawny są zobowiązani do odbycia szkolenia wstępnego na temat Rozporządzenia, ustawy o ochronie danych osobowych, Polityki oraz dokumentów powiązanych.

10.2.3. Zapoznanie się z ww. dokumentami pracownik/ osoba, z którą zawarto kontrakt cywilnoprawny potwierdza poprzez złożenie zobowiązania do zachowania poufności. Dokument ten podpisuje oprócz osoby składającej zobowiązanie IOD lub upoważniony pracownik Działu Służ Pracowniczych. Jeden egzemplarz zobowiązania otrzymuje IOD, drugi – pracownik/osoba, z którą zawarto kontrakt cywilnoprawny.

10.2.4. Każdy osoba, która będzie przetwarzała dane osobowe, otrzymuje w formie pisemnej upoważnienie do przetwarzania danych osobowych, które wydawane jest na czas trwania stosunku pracy/ stosunku cywilnoprawnego oraz stażu, w przypadku lekarzy stażystów. Pracownik otrzymuje upoważnienie nadawane przez Administratora danych na podstawie wniosku kierownika danej komórki organizacyjnej natomiast osoba zatrudniana na podstawie kontraktu cywilnoprawnego w dniu podpisania umowy, po złożeniu zobowiązania do zachowania poufności. Upoważnienie traci ważność z chwilą ustania stosunku umownego. Upoważnienie pracownika/ osoby świadczącej pracę na podstawie kontraktu cywilnoprawnego jest przechowywane wraz z wnioskiem i zobowiązaniem do zachowania poufności w dokumentacji IOD.

10.2.5. Wszyscy pracownicy Szpitala oraz osoby zatrudnione na podstawie kontraktu cywilnoprawnego podlegają szkoleniu wstępnemu oraz szkoleniom okresowym - stosownie do potrzeb wynikających ze zmian w systemie zabezpieczeń danych osobowych i zastosowania nowych sposobów, środków i form ich ochrony oraz w związku ze zmianą przepisów prawa powszechnie obowiązującego oraz przepisów wewnętrznych dotyczących ochrony danych osobowych. Karta szkolenia wstępnego z zakresu ochrony danych osobowych stanowi załącznik Nr 10 do Polityki.

10.2.6. Studenci i praktykanci odbywający szkolenia i praktyki w Szpitalu składają zobowiązania do zachowania poufności – Załącznik Nr 5 do Polityki;

10.2.7. Istnieje możliwość modyfikowania upoważnień i uprawnień do dostępu do danych osobowych. Czynność ta może nastąpić w wyniku zmiany zadań i obowiązków służbowych użytkownika, w szczególności zmiany komórki organizacyjnej, w której dana osoba pracuje

lub, na której rzecz wykonuje zadania oraz w przypadku gdy zajdą inne przyczyny zmiany nadanych uprawnień. W razie ustania zatrudnienia Administrator danych odbiera upoważnienie do przetwarzania danych osobowych. Wzory modyfikacji upoważnienia i odebrania upoważnienia do przetwarzania danych osobowych stanowią odpowiednio Załączniki Nr 8 i Nr 9 do Polityki.

10.3. Szkolenia w zakresie ochrony danych osobowych

10.3.1. Szkolenie organizuje się w formie szkolenia wstępnego i okresowego;

10.3.2. W szkoleniu wstępnym uczestniczą wszyscy nowo przyjęci pracownicy i osoby zatrudnione na podstawie umowy cywilnoprawnej. W ramach szkolenia zostają zapoznani z Rozporządzeniem, ustawą o ochronie danych osobowych, Polityką oraz dokumentami powiązanymi;

10.3.3. Szkoleniu wstępnemu podlegają także stażyści, osoby odbywający specjalizacje, w tym staże cząstkowe, studenci oraz praktykanci w ramach praktyk studenckich odbywających się w Szpitalu;

10.3.4. Okresowe szkolenia organizuje się w szczególności w celu zapoznania wszystkich pracowników Szpitala ze zmianami w obowiązujących przepisach w zakresie ochrony danych osobowych oraz zmianami w prowadzonej dokumentacji dotyczącej ochrony danych osobowych;

10.3.5. Przekazywanie materiałów szkoleniowych może odbywać się także za pośrednictwem Intranetu (e - szkolenia).

11. Podmioty odpowiedzialne za ochronę danych osobowych

Za ochronę danych osobowych przetwarzanych w Szpitalu odpowiadają:

1) Administrator danych (ADO)- zadania i obowiązki zostały określone w pkt 5;
2) Inspektor Ochrony Danych (IOD)- zadania i obowiązki zostały określone w pkt 5;
3) Administrator Bezpieczeństwa Systemów Informatycznych (ABSI);
4) Lokalny Administrator Systemów Informatycznych (LAIT);
5) Lokalny Administrator Zbiorów Danych Osobowych (LAZDO);
6) pracownicy i osoby świadczący pracę w ramach umów cywilno-prawnych;
7) podmioty przetwarzające na podstawie zawartych umów powierzenia przetwarzania danych osobowych.

11.1. **Do zadań Administratora Bezpieczeństwa Systemów Informatycznych (ABSI)** należy kontrola nad ochroną i bezpieczeństwem systemów informatycznych, a w szczególności**:**

1) bieżąca kontrola przestrzegania procedur bezpieczeństwa teleinformatycznego;
2) sprawowanie nadzoru nad technologiczną prawidłowością użytkowania systemów;
3) podejmowanie działań sprawdzających, kontrolnych lub zapobiegawczych mających na celu zapewnienie należytego poziomu bezpieczeństwa teleinformatycznego;
4) reagowanie na incydenty bezpieczeństwa teleinformatycznego;
5) w przypadku naruszenia przepisów bezpieczeństwa teleinformatycznego w Szpitalu, identyfikowanie i analiza zagrożeń bezpieczeństwa teleinformatycznego oraz podejmowanie działań zmierzających do ich zminimalizowania;
6) szkolenie pracowników Szpitala w zakresie bezpieczeństwa teleinformatycznego;
7) nadzór nad prowadzeniem ewidencji osób uprawnionych do pracy w systemach informatycznych, którą prowadzą Lokalni Administratorzy Systemów Informatycznych (LAIT);
8) współpraca z IOD w zakresie opracowania i aktualizacji dokumentacji przetwarzania danych osobowych, w szczególności rejestru czynności przetwarzania danych osobowych, rejestru kategorii przetwarzania oraz analizy ryzyka i oceny skutków dla ochrony danych osobowych.

11.2. **Do zadań Lokalnych Administratorów Systemów Informatycznych (LAIT)** należy w szczególności:

1) na podstawie zatwierdzonego wniosku o nadanie / modyfikację uprawnień do systemów informatycznych**:**

   aa) przeszkolenie osoby z zakresu bezpieczeństwa informatycznego, obsługi komputera oraz systemów informatycznych;

   bb) utworzenie konta, identyfikatora i pierwotnego hasła użytkownika oraz nadanie uprawnień do systemów informatycznych;
2) dbanie o bezpieczeństwo systemów i danych w nich zawartych, nadzorowanie, wykrywanie i eliminowanie nieprawidłowości;
3) asystowanie i współpraca z zewnętrznymi specjalistami przy pracach instalacyjnych, konfiguracyjnych i naprawczych.

11.3. **Do zadań Lokalnych Administratorów Zbiorów Danych Osobowych (LAZDO)** należy w szczególności:

1) wnioskowanie do ADO o dostęp do danych osobowych i do systemów informatycznych lub ich modyfikację dla nowych i aktualnych pracowników oraz innych osób wykonujących zadania w podległej komórce organizacyjnej;
2) zapoznanie nowych pracowników z powszechnie obowiązującymi przepisami w zakresie ochrony danych osobowych Polityką, Instrukcją „Zarządzanie systemem informatycznym w zakresie ochrony danych osobowych" oraz Instrukcją „Postępowanie w przypadku naruszenia ochrony danych osobowych";
3) współpraca z IOD w zakresie w identyfikacji zbiorów danych osobowych oraz czynności przetwarzania danych osobowych;
4) określenie indywidualnych obowiązków i odpowiedzialności osób zatrudnionych przy przetwarzaniu danych osobowych;
5) zapewnienie w podległych komórkach organizacyjnych warunków ochrony i bezpieczeństwa danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osoby nieuprawnione, przetwarzaniem z naruszeniem ochrony danych, utratą, uszkodzeniem lub zniszczeniem;
6) zgłaszanie IOD potrzeby zawarcia z innym podmiotem umowy przetwarzania danych osobowych w przypadku:

   a) umowy zakupu wyrobów medycznych połączonych z dzierżawą / użyczeniem sprzętu medycznego z nośnikiem danych osobowych np. analizatory, aparat ultrasonograficzny itp.;

   b) otrzymania w ramach testowania aparatury/ sprzętu medycznego z nośnikami danych osobowych;
7) nadzór nad poprawnością merytoryczną danych gromadzonych w systemach informatycznych;
8) wykonywanie zaleceń IOD i ABSI w zakresie ochrony danych osobowych.

11.4. **Zadania personelu - pracowników/ osób świadczących pracę w ramach umów cywilnoprawnych upoważnionych do przetwarzania danych osobowych.**

11.4.1.Dostęp do danych osobowych pacjentów posiada personel medyczny (w szczególności lekarze oraz pielęgniarki) oraz inne osoby wykonujące czynności pomocnicze niezbędne przy udzielaniu świadczeń zdrowotnych, adekwatnie do ich obowiązków służbowych i zgodnie upoważnieniem do przetwarzania danych osobowych.

11.4.2.Personel Administratora danych zobowiązany jest do:

1) zapoznania się, stosowania przepisów prawa w zakresie ochrony danych osobowych, w tym Rozporządzenia, a także do udziału w szkoleniach w tym zakresie;

2) ochrony przetwarzanych danych osobowych przed nieuprawnionym dostępem do tych danych, ich nieuzasadnioną modyfikacją lub zniszczeniem, jeżeli nie podlegają archiwizacji;

3) niszczenia w bezpieczny sposób wszelkich nośników zawierających dane osobowe (w formie papierowej jak i elektronicznej);

4) korzystania z zasobów informatycznych oraz sprzętu w sposób zgodny z ich przeznaczeniem i w sposób bezpieczny, m.in. poprzez okresową zmianę haseł, zachowanie poufności loginów i haseł oraz niepozostawianie sprzętu bez nadzoru;

5) niezwłocznego informowania przełożonych o zaobserwowanych nieprawidłowościach, które mogą mieć wpływ na bezpieczeństwo przetwarzanych danych osobowych;

6) przechowywania dokumentacji zawierającej dane osobowe w przeznaczonych do tego miejscach, z ograniczonym dostępem osób trzecich, zwłaszcza dokumentacji medycznej pacjentów;

7) niepozostawiania stanowisk recepcyjnych/punktów rejestracji pacjenta bez nadzoru;

8) noszenia identyfikatorów;

9) zachowania w tajemnicy danych osobowych, środków i sposobów ich zabezpieczenia w trakcie trwania stosunku pracy/stosunku cywilnoprawnego oraz po ich ustaniu.

11.4.3. Personel ponosi odpowiedzialność za należyte wykonywanie swoich obowiązków i jest pouczony przez Administratora danych o sankcjach wynikających z nieprawidłowości w tym zakresie, w tym o odpowiedzialności karnej.

12**. Dostęp do danych osobowych w systemach informatycznych**

Każdy nowo zatrudniony pracownik bez względu na formę zatrudnienia, lub inna osoba zgodnie z zawartą umową cywilnoprawną, przed dopuszczeniem do pracy powiązanej z obsługą systemów informatycznych podlega przeszkoleniu przez Lokalnego Administratora Systemów Informatycznych(LAIT) w zakresie obsługi komputera i korzystania z systemów informatycznych zgodnie z nadanymi uprawnieniami, uzyskuje identyfikator użytkownika, hasło i uprawnienia do dostępu do systemu/ów informatycznego /ych oraz odbywa szkolenie na stanowisku pracy z użytkowania programów komputerowych i aplikacji stosowanych

w poszczególnych komórkach organizacyjnych - szkolenie prowadzi Lokalny Administrator Zbiorów Danych Osobowych (LAZDO) lub osoba przez niego upoważniona, w razie potrzeby - przy udziale pracownika Sekcji Informatycznej i Telekomunikacji.

13. **Zasady powierzania przetwarzania danych osobowych podmiotom zewnętrznym**

13.1. Administrator danych może korzystać z usług podmiotów zewnętrznych w celu wspierania administratora w jego bieżącej działalności, w szczególności polegającej na dostarczeniu oraz/lub utrzymaniu infrastruktury teleinformatycznej, w tym narzędzi wspierających administratora w prowadzeniu dokumentacji medycznej w formie elektronicznej.

13.2. Administrator danych korzysta wyłącznie z usług takich dostawców usług, którzy zapewniają odpowiednie gwarancje bezpieczeństwa danych osobowych i zgodności przetwarzania danych z przepisami Rozporządzenia.

13.3.W tym celu Administrator danych zawiera z podmiotem zewnętrznym (podmiotem przetwarzającym) umowę powierzenia przetwarzania danych osobowych lub reguluje okoliczność powierzenia przetwarzania danych innym instrumentem prawnym.

13.4. Umowa powierzenia powinna określać zakres i cel przetwarzania danych osobowych. Zakres przetwarzania obejmuje kategorie danych osobowych oraz operacje, jakie podmiot przetwarzający może wykonywać na powierzonych mu danych osobowych. Określenie celu to wskazanie realizacji usług będących przedmiotem umowy głównej;

13.5. Podmiot przetwarzający przed rozpoczęciem przetwarzania danych zobowiązany jest podjąć środki zabezpieczające powierzone dane osobowe;

13.6. Nadzór merytoryczny nad realizacją umów powierzenia przetwarzania danych osobowych, oprócz Inspektora Ochrony Danych sprawują:

1) kierownik Sekcji Sprzętu Medycznego we współpracy z Administratorami Zbiorów Danych Osobowych (LAZDO) - w zakresie aparatury i sprzętu medycznego;
2) kierownik Sekcji Informatyki i Telekomunikacji - w ramach urządzeń, sprzętu informatycznego i kopiującego;
3) kierownicy innych komórek organizacyjnych stosownie do przedmiotu umowy głównej.

13.7. Inspektor Ochrony Danych prowadzi rejestr umów powierzenia przetwarzania danych osobowych - Załącznik Nr 13 do Polityki. Wzór umowy powierzenia przetwarzania danych osobowych stanowi Załącznik Nr 12 do Polityki.

14. Analiza ryzyka i ocena skutków dla ochrony danych osobowych. Zabezpieczenie danych osobowych

14.1. Analizę ryzyka opartą na ryzyku i ocenę skutków dla ochrony danych osobowych przeprowadza się nie mniej niż raz w roku, przy każdej istotnej zmianie systemu oraz w przypadku stwierdzenia incydentów.

14.2. Dla prawidłowego przeprowadzenia analizy ryzyka i oceny skutków istotne jest właściwe nadanie priorytetów określonym zagrożeniom oraz poprawne oszacowanie podatności istniejących w danym systemie zasobów na konkretne zagrożenie. Wyróżniamy:

1) **Zagrożenia naturalne -** pożar, zalanie, uderzenie pioruna, zawalenie się struktury budynku, duża wilgotność i temperatura, zanieczyszczenie powietrza, zakłócenia źródła zasilania itp.
2) **Zagrożenia losowe-** błędy i pomyłki administratorów, zaniedbania użytkowników, defekty oprogramowania, awarie sprzętu itp.
3) **Zagrożenia celowe:**
   a) **aktywne -** przełamanie haseł dostępu, metody socjotechniczne pozyskiwania informacji, fałszowanie i kasowanie zbiorów, użycie złośliwego oprogramowania, wyłudzenie, kradzież i fałszowanie dokumentów, nośników, kluczy, haseł, wykorzystanie promieniowania ujawniającego, manipulowanie informacją przesyłaną siecią (modyfikacja informacji, usuwanie komunikatów, opóźnianie komunikatów, przekierowywanie informacji, maskarada, odcięcie kanału transmisyjnego itp.
   b) **pasywne** - wyparcie się nadania komunikatu, wyparcie się odbioru komunikatu, podgląd transmitowanych danych, obserwacja i analiza ruchu komunikatów w sieci, podsłuch sieciowy.

14.3. Zastosowane środki bezpieczeństwa

W celu zapewnienia bezpieczeństwa danych osobowych oraz urządzeń i systemów informatycznych, w których dane są przetwarzane, odpowiednio do zagrożeń oraz kategorii tych danych objętych ochroną, w szczególności w celu zabezpieczenia ich przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem wprowadzono strefy bezpieczeństwa i środki bezpieczeństwa.

W każdej ze strefy bezpieczeństwa wzięto pod uwagę następujące parametry:

1) podstawowe kryteria i sposób określania poziomu zagrożeń;

2) dobór środków bezpieczeństwa fizycznego odpowiednich do wskazanego poziomu zagrożeń;
3) rodzaje zagrożeń, które należy uwzględnić przy określaniu poziomu zagrożeń;
4) podstawowe elementy, które powinien zawierać plan ochrony informacji;
5) zakres stosowania środków bezpieczeństwa fizycznego;
6) kryteria tworzenia stref ochronnych.

Celem zastosowania środków bezpieczeństwa jest:

1) zapewnienie właściwego przetwarzania informacji;
2) umożliwienie zróżnicowania dostępu do informacji niejawnych dla pracowników zgodnie z posiadanymi przez nich uprawnieniami oraz uzasadnioną potrzebą dostępu do informacji;
3) wykrywanie, udaremnianie lub powstrzymywanie działań nieuprawnionych;
4) uniemożliwianie lub opóźnianie wtargnięcia osób nieuprawnionych, w sposób niezauważony lub z użyciem siły, do pomieszczenia lub obszaru, w którym są przetwarzane informacje niejawne.

Zastosowane środki bezpieczeństwa pogrupowano w trzy kategorie dotyczące:

1) zabezpieczeń fizycznych;
2) zabezpieczeń technicznych;
3) zabezpieczeń proceduralno - organizacyjnych.

Ad.1. Zabezpieczenia fizyczne obejmują takie elementy jak: ochrona poszczególnych, wybranych pomieszczeń, ochrona sprzętu informatycznego, wydzielenie stref bezpieczeństwa i administracyjnych, dozór fizyczny, systemy alarmowe, systemy wizyjne, systemu kontroli dostępu itd.

Każda z form ochrony fizycznej jest dostosowana do wartości chronionej i tak, aby nakłady przeznaczone na wdrożenie zabezpieczeń nie były wyższe niż wartość chroniona.

Środki bezpieczeństwa fizycznego stosuje się we wszystkich pomieszczeniach i obszarach, w których są przetwarzane informacje.

Ad.2. Zabezpieczenia techniczne łączą się bezpośrednio ze sprzętem informatycznym i oprogramowaniem, oznaczają, np. szyfrowanie danych, sprzętową lub programową detekcję intruzów w systemie, weryfikację integralności danych, czy bezpieczeństwo kanałów transmisyjnych.

Ad.3. Zabezpieczenia proceduralno- organizacyjne:

1) opracowanie i wdrożenie Polityki danych osobowych;
2) opracowanie i wdrożenie Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
3) Dopuszczenie do przetwarzania danych osobowych wyłącznie osób upoważnionych z mocy ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta oraz osoby, którym upoważnienie nadał Administrator danych;
4) opracowanie i wdrożenie procedury postępowania w przypadku naruszenia ochrony danych osobowych;
5) szkolenie osób przetwarzających dane osobowe w zakresie przepisów o ochronie danych osobowych i zabezpieczeń systemu informatycznego;
6) przetwarzanie danych osobowych jest dokonywane w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;
7) przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych;
8) dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonując takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści, aby po dokonaniu usunięcia danych niemożliwa była identyfikacja osób.

14.4. **W Szpitalu wyznaczono trzy strefy bezpieczeństwa:**

1) **I Strefa bezpieczeństwa**

Strefa, w której następuje bezpośredni kontakt pracownika Szpitala z pacjentem/klientem. Odbywa się w niej bezpośrednie wprowadzanie niezbędnych informacji do zbiorów danych osobowych. Gromadzenie i przechowywanie danych w tej strefie ogranicza się do czasu niezbędnego do wykonania czynności służbowych.

W pomieszczeniach tej strefy wydziela się dwa obszary:

A – obszar, w którym mogą przebywać osoby nieupoważnione do przetwarzania danych osobowych.

B – obszar, w którym przetwarza się dane osobowe.

W obszarze B Komputery	Komputery są ustawione w sposób uniemożliwiający wgląd osobom nieupoważnionym do przetwarzania danych osobowych na zawartość wyświetloną na ekranie monitora. W przypadku gdy osoba nieupoważniona ma możliwość podejrzenia informacji zawartych na ekranie monitora, pracownik niezwłocznie powinien

	zawiesić pracę w systemie (zminimalizowanie wszystkich okien poprzez naciśnięcie ikony pulpitu na pasku zadań), do czasu załatwienia sprawy.
W obszarze B Dokumenty	Ilość dokumentów na biurkach ogranicza się do dokumentów niezbędnych do pracy w danej chwili. Pozostałe dokumenty przechowywane są w szafkach zamykanych na klucz. Wszelkie dane są wprowadzane do ksiąg i kartotek w sposób uniemożliwiający wgląd w dane osobom nieupoważnionym.
Zabezpieczenie pomieszczeń	Zamki w drzwiach.

2) **II Strefa bezpieczeństwa**

Strefa, gdzie są gromadzone, przechowywane i opracowywane większe ilości danych osobowych do czasu ich archiwizacji. W tej strefie odbywa się wymiana informacji pomiędzy pracownikami Szpitala. Zasady pracy i wymiana danych w strefie II podlegają tym samym regułom jak w I strefie.

W obszarze B Komputery	Komputery są ustawione w sposób uniemożliwiający podgląd osobom nieupoważnionym do przetwarzania danych osobowych na zawartość wyświetloną na ekranie monitora. W przypadku, gdy osoba nieupoważniona ma możliwość podejrzenia informacji zawartych na ekranie monitora, pracownik niezwłocznie powinien zawiesić pracę w systemie (zminimalizowanie wszystkich okien poprzez naciśnięcie ikony pulpitu na pasku zadań), do czasu załatwienia sprawy.
W obszarze B Dokumenty	Ilość dokumentów na biurkach ogranicza się do dokumentów niezbędnych do pracy w danej chwili. Pozostałe dokumenty przechowywane są w szafkach kartotecznych zamykanych na klucz, odpowiednich regałach oraz inne wyposażenie, które określone jest odpowiednimi przepisami prawa. Wszelkie dane są wprowadzane do ksiąg i kartotek w sposób uniemożliwiający wgląd w dane osobom nieupoważnionym. Dokumenty zawierające dane osobowe przechowywane są w sposób uniemożliwiający ich zniszczenie, bądź narażenie Szpitala na utratę zaufania.
Zabezpieczenie pomieszczeń	Pomieszczenia dodatkowo zabezpiecza się w techniczne i fizyczne środki ochrony przewidziane Planem Ochrony Szpitala.

3) **III Strefa bezpieczeństwa**

Strefa, w której archiwizowane są wszelkie zbiory danych osobowych wytworzone w Szpitalu oraz pomieszczenia, w których znajdują się ważne urządzenia i środki techniczne służące do przetwarzania danych osobowych.

Dostęp do w pomieszczeń III strefy bezpieczeństwa posiadają:

1) pracownicy upoważnieni do pracy w III strefie bezpieczeństwa np. pracownicy Sekcji Informatyki i Telekomunikacji, Kasy Głównej Szpitala, Archiwum Zakładowego;
2) Kadra zarządzająca Szpitala;
3) Inspektor Ochrony Danych, Administrator Bezpieczeństwa Systemów Informatycznych;
4) inni pracownicy na podstawie upoważnienia Administratora Danych.

Osoby wymienione w punkcie 2-4 mogą przebywać w tych pomieszczeniach tylko w obecności użytkowników tych pomieszczeń.

Wszystkie pomieszczenia III strefy bezpieczeństwa są wyposażone w środki ochrony o podwyższonej klasie bezpieczeństwa.

Za aktualizację stref bezpieczeństwa i środków bezpieczeństwa odpowiada pełnomocnik Dyrektora ds. Ochrony Informacji Niejawnych i Obrony Cywilnej przy współpracy z Kierownikiem Sekcji Inwestycji i Remontów oraz Kierownikiem Działu Technicznego.

14.5. Ocena skutków dla ochrony danych

14.5.1.Administrator danych przeprowadza ocenę skutków dla ochrony danych i dokumentuje fakt dokonania tej oceny.

14.5.2.Wykonanie oceny skutków dla ochrony danych jest konieczne, jeżeli dany rodzaj przetwarzania - w szczególności z użyciem nowych technologii - ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw i wolności pacjentów. Dla podobnych operacji przetwarzania wiążących się z podobnym wysokim ryzykiem ocena skutków dla ochrony danych wykonywana jest pojedynczo.

14.5.3.Wykonanie oceny skutków dla ochrony danych osobowych jest wymagane w szczególności w przypadku:

1) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie wykorzystującego elementy rozpoznawania cech lub właściwości obiektów znajdujących się w monitorowanej przestrzeni, z użyciem danych pacjentów, prowadzonego przez szpital, podmiot prowadzący badania kliniczne lub pobierający materiał genetyczny do badań;

2) przetwarzania na dużą skalę informacji o stanie zdrowia, w szczególności dokonywane przez szpital lub placówkę medyczną.

14.5.4.Administrator danych monitoruje wykaz rodzajów przetwarzania, dla których wymagane jest przeprowadzenie oceny skutków dla ochrony danych opublikowany przez UODO i dokonuje oceny skutków czynności przetwarzania wskazanych w tym wykazie jako rekomendowanych do poddania tej ocenie.

14.5.5.Ocena skutków dla ochrony danych osobowych zawiera co najmniej:

1) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie - prawnie uzasadnionych interesów realizowanych przez administratora;

2) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celu, w jakim dane zostały pozyskane;

3) ocenę ryzyka naruszenia praw i wolności pacjentów;

4) środki planowane w celu mitygacji ryzyka, w tym zabezpieczenia, środki i mechanizmy bezpieczeństwa zapewniające ochronę danych oraz wykazanie przestrzegania przepisów Rozporządzenia;

14.5.6.Administrator danych dokonuje bieżącego przeglądu czynności przetwarzania, o których mowa w pkt 5.7.-5.10. celem weryfikacji, czy przetwarzanie to odbywa się w sposób zgodny z dokonaną oceną skutków dla ochrony danych osobowych.

14.5.7.Administrator danych konsultuje się z UODO, jeżeli dokonana ocena skutków dla ochrony danych będzie wskazywała na występowanie wysokiego ryzyka dla praw i wolności pacjentów, jeżeli nie zastosowane zostałyby środki mitygujące ryzyko. Konsultacje z UODO dokonywane są przed rozpoczęciem przetwarzania danych osobowych.

14.6. Pracownicy i inne osoby (użytkownicy), którym nadano dostęp do przetwarzania danych osobowych i do systemów komputerowych ponoszą odpowiedzialność za:

1) jakość wprowadzania danych osobowych, jeżeli dokonuje rejestracji lub je przetwarza;
2) zapewnienie bezpieczeństwa i poufności wszelkich dokumentów w czasie użytkowania;
3) zabezpieczenie wszystkich informacji zawierających dane osobowe przechowywane poza systemem informatycznym (na lokalnych stacjach roboczych, w pojedynczych plikach lub katalogach) przed nieuprawnionym dostępem poprzez zastosowanie haseł lub zabezpieczeń kryptograficznych;

4) prowadzenie ewidencji, jakie dane osobowe, kiedy i komu zostały przekazane.

Zabrania się wynoszenia poza teren Szpitala dokumentów i elektronicznych nośników informacji zawierających dane osobowe;

Odpowiedzialność za ochronę i bezpieczeństwo przetwarzania danych osobowych ponosi każdy pracownik/osoba świadcząca pracę na podstawie kontraktu cywilnoprawnego zgodnie z powierzonym zakresem zadań wskazanym w:

a) Karcie zadań, uprawnień i odpowiedzialności lub zawartej umowie cywilnoprawnej;
b) Regulaminie pracy Wojewódzkiego Szpitala Zespolonego w Elblągu.

15. Dokumenty powiązane z Polityką Bezpieczeństwa danych osobowych:

1) Plan ochrony Wojewódzkiego Szpitala Zespolonego w Elblągu;
2) Wykaz aparatury/ sprzętu medycznego będącego na stanie Wojewódzkiego Szpitala Zespolonego w Elblągu;
3) Zasady przeglądów i konserwacji urządzeń, aparatury i sprzętu w ciągłej pracy;
4) Dokumentacja Zintegrowanego Systemu Zarządzania związana z obszarem bezpieczeństwa ochrony danych osobowych.

16. Postanowienia końcowe

16.1. Politykę ochrony danych osobowych otrzymują:

1) Sekcja Zarządzania Jakością
2) Inspektor Ochrony Danych – kopię na prawach oryginału.

16.2. Polityka Ochrony danych osobowych, Instrukcja - Zarządzanie systemem informatycznym w zakresie ochrony danych osobowych oraz Instrukcja „Postępowanie w przypadku naruszenia ochrony danych osobowych" są dostępne dla wszystkich pracowników/ osób świadczących pracę na podstawie kontraktu cywilnoprawnego, w sieci informatycznej Szpitala (Intranet) z wyjątkiem Wykazu budynków i pomieszczeń, w których przetwarzane są dane osobowe, opatrzonego klauzulą „ Zastrzeżone".

Sporządził: Zatwierdził:

Elbląg, dnia 15 października 2018 r.