Polityka Bezpieczeństwa Informacji Szpitala Specjalistycznego im. Jędrzeja Śniadeckiego w Nowym Sączu

Załącznik nr 1 do Zarządzenia nr 85 z dnia 24.05.2018 r.
Dyrektora Szpitala Specjalistycznego im. Jędrzeja Śniadeckiego
w Nowym Sączu w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji

Szpital Nowy Sącz 1906	***Szpital Specjalistyczny im. Jędrzeja Śniadeckiego w Nowym Sączu ul. Młyńska 10 33-300 Nowy Sącz***	***Wydanie: 4***
		Obowiązuje od dnia- 25.05.2018 r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI Szpitala Specjalistycznego im. Jędrzeja Śniadeckiego w Nowym Sączu

Sporządził: ***Inspektor Ochrony Danych***	***Sprawdził:*** ***Administrator Systemu Informatycznego***	***Zatwierdził:*** ***p.o. Dyrektor***
Anna DĄBROWSKA	**Arkadiusz SZCZECINA**	**Lidia ZELEK**
Podpis: Dąbrowska Anna	Podpis: ADMINISTRATOR Systemów Informatycznych Arkadiusz Szczecina	Podpis: p.o. DYREKTORA Szpitala Specjalistycznego im. Jędrzeja Śniadeckiego w N.Sączu Lidia Zelek

ROZDZIAŁ I Wprowadzenie

Polityka Bezpieczeństwa Informacji zwana dalej „**Polityką**", stanowi najwyższej rangi dokument zawierający zasady dotyczące ochrony danych osobowych przetwarzanych w Szpitalu Specjalistycznym im. Jędrzeja Śniadeckiego w Nowym Sączu. **Politykę** stosuje się do wszystkich przetwarzanych danych bez względu na miejsce, formę czy sposób przetwarzania, dla których Szpital jest administratorem oraz do danych powierzonych do przetwarzania.

Polityka obowiązuje wszystkie osoby przetwarzające dane osobowe w imieniu Szpitala. Stosowanie zasad określonych w **Polityce** ma na celu zapewnienie prawidłowej ochrony danych osobowych przetwarzanych w Szpitalu, rozumianej jako ochrona danych przed ich nieuprawnionym udostępnieniem, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych bądź utratą, uszkodzeniem lub zniszczeniem.

Polityka została opracowana na podstawie obowiązujących aktów prawnych, m.in.:
- 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. U. UE.L.2116/119/1)- dalej: RODO;
- Ustawy o ochronie danych osobowych;
- Ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej (t.j. Dz. U. z 2018 r. poz. 160 z późn.zm.).
- Ustawy z 06.11.2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (t.j. Dz. U. z 2017 r. ze zm.)

Zasady ochrony informacji niejawnych reguluje ustawa o ochronie informacji niejawnych oraz opracowane na jej podstawie inne wewnętrzne regulacje Szpitala.

ROZDZIAŁ II Definicje

1. ***„dane osobowe"*** oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); 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;
2. ***„przetwarzanie"*** oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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;
3. ***„administrator"*** - oznacza Szpital Specjalistyczny im. J. Śniadeckiego w Nowym Sączu (dalej: Szpital);

4. ***„podmiot przetwarzający”*** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
5. ***„odbiorca”*** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe;
6. ***„zgoda”*** osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
7. ***„naruszenie ochrony danych osobowych”*** oznacza 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;
8. ***„dane dotyczące zdrowia”*** oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej- w tym o korzystaniu z usług opieki zdrowotnej- ujawniające informacje o stanie jej zdrowia;
9. ***„organ nadzorczy”*** oznacza Urząd Ochrony Danych Osobowych (dawniej: GIODO);
10. ***„Inspektor Ochrony Danych /IOD/”***- osoba wyznaczona przez administratora odpowiedzialna za nadzorowanie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych;
11. ***„Administrator Systemów Informatycznych /ASI/”***- osoba wyznaczona przez administratora odpowiedzialna za funkcjonowanie systemu informatycznego;
12. ***„Lokalny Administrator Systemu /LAS/”*** - osoba wyznaczona przez administratora do przetwarzania danych osobowych w danym systemie oraz zarządzająca uprawnieniami do tego systemu;
13. ***„osoba upoważniona”*** - osoba posiadająca pisemne upoważnienie wydane przez IOD, uprawniona do przetwarzania danych osobowych.

ROZDZIAŁ III Odpowiedzialność

1. Za bezpieczeństwo danych osobowych w Szpitalu odpowiadają:
1) Administrator – Dyrektor Szpitala;
2) Inspektor Ochrony Danych /IOD/;
3) Administrator Systemu Informatycznego /ASI/;
4) Lokalny Administrator Systemu /LAS/;
5) wszystkie osoby mające dostęp do danych osobowych.

Odpowiedzialność poszczególnych osób, określono w zakresach czynności oraz umowach.

ROZDZIAŁ IV Zasady dotyczące przetwarzania danych osobowych

1. Dane osobowe w Szpitalu przetwarza się:

1) Zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą. Każda osoba, której dane dotyczą, jest informowana o prowadzeniu operacji przetwarzania i o jej celach, przed ich zbieraniem. Informacje te są przekazywane w sposób zrozumiały, sformułowane jasnym i prostym językiem- zwłaszcza, gdy dotyczy to stanu zdrowia;
2) W przypadku danych dotyczących stanu zdrowia, zgoda nie jest pobierana. Pracownicy rejestracji zobowiązani są przed zebraniem danych do poinformowania pacjenta o

przysługujących mu: prawach, celach, sposobie przetwarzania oraz konsekwencjach nie podania danych osobowych (co zawarto w klauzuli informacyjnej). Pacjent jest także informowany, komu zgodnie z prawem Szpital może przekazać jego dane osobowe. Klauzule informacyjne zamieszcza się także na tablicach informacyjnych przy rejestracjach, oraz na stronie internetowej Szpitala.

2. W przypadku przetwarzania danych, na które wymagana jest zgoda, klauzule informacyjne i zgoda osoby, której dane dotyczą są umieszczane na dokumentach, dotyczących danego postępowania/ przetwarzania. Dane zebrane w konkretnych, wyraźnych i prawnie uzasadnionych celach, nie mogą być przetwarzane dalej w sposób niezgodny z tymi celami. Przetwarzanie do celów archiwalnych, badań naukowych i statystycznych nie jest uznawane za niezgodne z pierwotnymi celami.
3. Odpowiednie środki ochrony danych osobowych (techniczne i organizacyjne), określono w kolejnych rozdziałach Polityki, a dla poszczególnych zbiorów, w Rejestrze czynności przetwarzania danych osobowych (u IOD). Środki te są poddawane przeglądom i uaktualniane przez Inspektora Ochrony Danych oraz Administratora Systemów Informatycznych.
4. W przypadku tworzenia nowego zbioru czy wprowadzenia nowego sytemu, każdorazowo przed ich wprowadzeniem IOD dokonuje analizy ryzyka.
5. Wszystkie dane osobowe, (w szczególności dotyczące stanu zdrowia) przekazywane w sieci publicznej (internetowo - e-mail) muszą być szyfrowane.
6. W przypadku przesyłania danych do innego systemu informatycznego stosuje się pseudonimizację.
7. Należy dążyć do tego, aby systemy informatyczne, w których przetwarzane są dane osobowe posiadały certyfikaty jakości.
8. Zbierane dane muszą być ograniczone tylko do danych wymaganych prawem, niezbędnych do realizacji danego celu.
9. Osoby przetwarzające dane są obowiązane dołożyć starań, aby zebrane dane osobowe były prawidłowe, aktualne oraz przechowywane przez okres określony w przepisach prawa. Dane nieprawidłowe w świetle celów ich przetwarzania, są usuwane lub prostowane. Za aktualizację zebranych danych odpowiada kierownik komórki organizacyjnej, w której dane są przetwarzane.
10. W przypadku współadministrowania danymi osobowymi, wspólnie ustala się cele i sposoby przetwarzania, oraz zakresy odpowiedzialności dotyczące przetwarzania i ochrony tych danych. **Gdy dane osobowe przetwarza kilku współadministratorów**, **osoba której dane dotyczą, musi wyrazić zgodę na przetwarzanie jej danych (dotyczy m.in. danych przetwarzanych w Systemie Informacji Medycznej – SIM).**
11. Za bezpieczeństwo przetwarzanych danych osobowych w poszczególnych komórkach organizacyjnych Szpitala odpowiada każda osoba; która przetwarza dane osobowe. W szczególności jest ona zobowiązana chronić dane przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, w szczególności za pomocą określonych przez administratora środków technicznych lub organizacyjnych.

ROZDZIAŁ V Przetwarzanie szczególnych kategorii danych osobowych

1. Dane dotyczące zdrowia, w tym dane genetyczne, mogą być przetwarzane, wyłącznie w celu świadczenia usług medycznych lub za pisemną zgodą właściciela danych.
2. Przetwarzanie danych genetycznych odbywa się zgodnie z procedurami określonymi w Medycznym Laboratorium Diagnostycznym.
3. W przypadku przetwarzania danych biometrycznych, osoba której dane dotyczą jest o tym informowana i na ich przetwarzanie musi wyrazić zgodę.
4. Nie jest wymagana zgoda do celów profilaktyki zdrowotnej lub medycyny pracy, oraz do oceny zdolności pracownika do pracy.

ROZDZIAŁ VI Prawa osoby, której dane dotyczą

1. Przejrzyste informowanie i przejrzysta komunikacja oraz tryb wykonywania praw przez osobę, której dane dotyczą

1) Szpital ułatwia osobie, której dane dotyczą, wykonanie praw jej przysługujących, chyba że wykaże, iż nie jest w stanie zidentyfikować tej osoby.
2) Wszelkie informacje dotyczące przetwarzania danych osobowych należy przekazać w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem, w formie pisemnej, ustnej lub elektronicznej.

2. Informacje i dostęp do danych osobowych

a) Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą

1) Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, to przed zebraniem danych osobowych, osoba zbierająca dane, podaje następujące informacje:
   a) swoją tożsamość i dane kontaktowe;
   b) dane kontaktowe inspektora ochrony danych;
   c) cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;
   d) wykaz osób przetwarzających dane;
   e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców;
   f) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
   g) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
   h) jeżeli przetwarzanie odbywa się na podstawie zgody, informacje o prawie do cofnięcia zgody w dowolnym momencie, bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
   i) informacje o prawie wniesienia skargi do organu nadzorczego;
   j) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych.

2) Powyższe informacje osoba zbierająca dane podaje ustnie; lub informuje właściciela danych gdzie może zapoznać się z tymi informacjami.

3) Informacje powyższe umieszcza się przy rejestracjach oraz na stronie internetowej Szpitala. Są one także dostępne w każdym sekretariacie i dyżurce pielęgniarskiej oraz u IOD.

b) Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą

Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są nie od tej osoby, (np. gdy pacjent jest nieprzytomny), to niezwłocznie po odzyskaniu przytomności (świadomości) należy jej przekazać powyższe informacje a także poinformować o źródle pochodzenia danych osobowych.

3. Prawo dostępu przysługujące osobie, której dane dotyczą

Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące. Ma także prawo dostępu do swoich danych oraz do otrzymania kopii swoich danych.

4. ***Prawo do sprostowania danych***

Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych oraz ma prawo żądania uzupełnienia niekompletnych danych osobowych; poprzez przedstawienie dodatkowego dokumentu czy oświadczenia.

Pacjent ma prawo zażądać niezwłocznego sprostowania lub uzupełnienia danych osobowych zawartych w dokumentacji medycznej wyłącznie w zakresie w jakim nie będzie prowadzić to do naruszenia autonomii zawodowej osoby wykonującej zawód medyczny, która dokonywała wpisu do dokumentacji medycznej.

5. Prawo do usunięcia danych („prawo do bycia zapomnianym")

1) Prawo do usunięcia danych nie dotyczy przetwarzania zgodnego prawem, przed upływem okresu ich przechowywania.

2) Prawo do usunięcia danych (do bycia zapomnianym) nie znajduje zastosowania wobec danych osobowych przetwarzanych w ramach dokumentacji medycznej, przez cały okres wymagany przepisami prawa, w tym archiwizacji dokumentacji medycznej.

6. Prawo do ograniczenia przetwarzania

1) Osoba, której dane dotyczą, ma prawo żądania od administratora ograniczenia przetwarzania danych osobowych ją dotyczących.

2) Jeżeli przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego.

3) Przed uchyleniem ograniczenia przetwarzania administrator informuje o tym osobę, której dane dotyczą, która żądała ograniczenia.

4) Pomimo żądania przez Pacjenta ograniczenia przetwarzania, w tym w szczególności wobec danych przetwarzanych w ramach dokumentacji medycznej można przetwarzać te dane w dotychczasowym zakresie, bowiem ograniczenie przetwarzania danych dokonywanego w celach zdrowotnych mogłoby istotnie utrudnić realizację tych celów (brak skuteczności ograniczenia przetwarzania w związku z ważnymi względami interesu publicznego).

7. Obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania

Administrator informuje o sprostowaniu, usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

8. Prawo do przenoszenia danych

Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, jeżeli:

a) przetwarzanie odbywa się na podstawie zgody,
b) na podstawie umowy,
c) przetwarzanie odbywa się w sposób zautomatyzowany.

9. ***Prawo do sprzeciwu oraz zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach***

1) Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją - wobec przetwarzania dotyczących jej danych osobowych w tym profilowania.

2) Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

ROZDZIAŁ VII Techniczne i organizacyjne środki ochrony danych osobowych

Szpital, uwzględniają ryzyko naruszenia praw lub wolności osób fizycznych i wdraża odpowiednie środki techniczne i organizacyjne zapewniające stopień bezpieczeństwa odpowiadający temu ryzyku, między innymi poprzez:

1) zapewnienie ochrony danych osobowych w oparciu o obowiązujące przepisy prawa i postanowienia PBI,
2) określenie zasad dostępu, przetwarzania i udostępniania danych osobowych,
3) minimalizowanie ryzyka w obszarze bezpieczeństwa fizycznego, teleinformatycznego, organizacyjno-prawnego oraz osobowego,
4) zaangażowanie wszystkich pracowników w ochronę danych osobowych oraz stałe podnoszenie umiejętności i kwalifikacji kadr w tej dziedzinie.

1. Zasady obowiązujące przy przetwarzaniu danych

1) Dane osobowe z użyciem systemu informatycznego i w formie papierowej są przetwarzane w Szpitalu całodobowo.
2) Przebywanie osób nieuprawnionych do dostępu do danych osobowych w pomieszczeniach znajdujących się wewnątrz obszaru przetwarzania tych danych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych.
3) Dokumentacja medyczna papierowa jak również tworzona w systemach informatycznych, we wszystkich komórkach organizacyjnych Szpitala powinna być przechowywana w sposób zapewniający poufność zawartych w niej danych, uniemożliwiający do niej dostęp osób nieupoważnionych oraz zabezpieczający przed zniszczeniem lub zgubieniem, a także umożliwiający jej wykorzystanie bez zbędnej zwłoki. Dokumentację należy przechowywać w szafach zamykanych na klucz.
4) Za prawidłowe przechowywanie dokumentacji i nieudostępnianie jej osobom nieupoważnionym odpowiedzialni są wszyscy pracownicy poszczególnych komórek organizacyjnych Szpitala. Sposób i miejsce przechowywania bieżącej dokumentacji wewnętrznej indywidualnej i zbiorczej, określają kierownicy/koordynatorzy komórek organizacyjnych Szpitala, zapewniając prawidłowe jej przetwarzanie i przechowywanie (w tym okres przechowywania zgodny z Instrukcją Kancelaryjną).
5) Należy szczególnie chronić dokumenty przenoszone poza obszarem przetwarzania danych.
6) Pomieszczenia w obszarze przetwarzania danych osobowych w czasie nieobecności pracowników są zamykane na klucz. Klucze są przechowywane w sposób uniemożliwiający dostęp do nich przez osoby nieupoważnione.
7) Monitory, na których odbywa się przetwarzanie danych osobowych są zlokalizowane w sposób uniemożliwiający osobom nieupoważnionym podgląd wyświetlanych danych.
8) Konfiguracja wyświetlania obrazu na monitorach komputerów musi zawierać włączenie wygaszacza ekranu po zadanym przez ASI czasie lub w przypadku braku wygaszacza ekranu wyłączenie monitora w przypadku braku, w określonym czasie aktywności użytkownika.
9) Dyski i inne nośniki elektroniczne zawierające dane osobowe przeznaczone do zniszczenia, naprawy lub przekazania są pozbawiane zapisu lub niszczone fizycznie (jeżeli nie ma innej metody zlikwidowania zapisu).
10) Wydruki komputerowe lub dokumenty błędnie sporządzone, zawierające dane osobowe, a przeznaczone do likwidacji są niszczone tak, aby nie było możliwości odczytania zamieszczonych na nich informacji.
11) W celu ochrony przed złośliwym oprogramowaniem stosuje się programy antywirusowe.

2. Ochrona przy zbieraniu i przekazywaniu danych

1) Przy rejestracji może znajdować się tylko jedna osoba. Jeśli jest to pacjent pierwszorazowy wskazane jest aby dane zbierać w wydzielonym miejscu.
2) Pacjentowi należy przekazywać dane, w miarę możliwości, tak aby nie słyszeli ich pozostali pacjenci.
3) W pomieszczeniach zarówno administracyjnych jak i sekretariatach i dyżurkach medycznych może znajdować się tylko jedna osoba załatwiająca sprawę.

Należy dopilnować aby nie było na biurkach, gdzie wchodzą osoby postronne, dokumentów z danymi osobowymi, w takiej odległości aby mogli je przeczytać czy zrobić zdjęcie.

4) Tam gdzie jest to możliwe należy ograniczyć wchodzenie osób postronnych do pomieszczeń.
5) Pacjentów, można wołać posługując się imieniem i nazwiskiem, jeśli wyrazili na to zgodę. Jeśli takiej zgody nie wyrazili należy używać imienia i przypisanego numeru.
6) Dane pracowników czy pacjentów przekazywane do innych działów np. do wysłania czy przekazania do ZUS mają być w zaklejonej i zaadresowanej kopercie.

3. Upoważnienia do przetwarzania danych osobowych

1) Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby, które zostały przeszkolone z zasad ochrony danych osobowych oraz podpisały stosowne oświadczenie o zachowaniu w tajemnicy przetwarzanych danych osobowych i otrzymały upoważnienie.
2) Dostęp do danych osobowych jest przyznawany zgodnie z zasadą wiedzy koniecznej – rzeczywiście wykonywanymi czynnościami. Nie można nadać stałego upoważnienia jeśli jakieś czynności mogą być lub są wykonywane sporadycznie. W takich sytuacjach każdorazowo nadaje się stosowne upoważnienie.
3) Osoby upoważnione do przetwarzania danych osobowych zobowiązane są zapoznania się i stosowania regulacji wewnętrznych dotyczących ochrony danych osobowych w Szpitalu.
4) Dane osobowe powinny być chronione przed nieuprawnionym dostępem i modyfikacją.
5) Dane osobowe zawarte w systemach informatycznych należy przetwarzać wyłącznie za pomocą autoryzowanych programów.
6) Upoważnienia są nadawane indywidualnie przed rozpoczęciem przetwarzania danych osobowych, przez IOD, a w czasie jego nieobecności przez ASI. Wydanie upoważnienia oraz rejestracja użytkownika systemu informatycznego przetwarzającego dane osobowe następuje na podstawie Karty obiegowej- zatrudnienia, a w szczególnych sytuacjach, na pisemny lub ustny wniosek bezpośredniego przełożonego.
7) Za przydzielenie i wygenerowanie identyfikatora /loginu/ oraz hasła użytkownikowi, który pierwszy raz będzie korzystał z systemu informatycznego, odpowiada ASI/ LAS odpowiedniego systemu informatycznego.
8) Hasło ustanowione podczas przyznawania uprawnień przez Administratora odpowiedniego systemu informatycznego należy zmienić na indywidualne po pierwszym poprawnym zalogowaniu się do sytemu. Zmiany hasła należy dokonywać co najmniej, co 30 dni.
9) Pracownicy są odpowiedzialni za zachowanie w tajemnicy swoich identyfikatorów i haseł.
10) Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
11) W sytuacji, kiedy zachodzi podejrzenie, że ktoś poznał hasło, pracownik zobowiązany jest do natychmiastowej zmiany hasła i poinformowania o tym fakcie IOD i ASI lub LAS.
12) Przy wyborze hasła obowiązują następujące zasady:

- minimalna długość hasła 8 znaków,
- zakazuje się stosować:

- haseł, które użytkownik stosował uprzednio,

- swojego imienia, drugiego imienia, nazwiska, przezwiska, pseudonimu w jakiejkolwiek formie, imion (w szczególności imion osób z najbliższej rodziny),
- ogólnie dostępnych informacji o użytkowniku (numer telefonu, numer rejestracyjny samochodu, numer PESEL, itp.),

- należy stosować:
    - hasła zawierające kombinacje liter i cyfr,
    - hasła zawierające znaki specjalne (.,():'@,#,& itp.) o ile system informatyczny i oprogramowanie na to pozwala,
    - zmiany hasła nie wolno zlecać innym osobom.

13) Pracownik ma prawo do wykonywania tylko tych czynności, do których został upoważniony. W sytuacjach szczególnych, jeśli dotyczy to bezpośrednio udzielania świadczeń medycznych, można przekazać dokumentację innej osobie wykonującej zawód medyczny lub instytucjom zgodnie z przepisami prawa.
14) Pracownik ponosi odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora /loginu/ i hasła dostępu.
15) Wyrejestrowanie użytkownika z systemu informatycznego może nastąpić: na podstawie Karty obiegowej- zwolnienia, na wniosek administratora danych; na wniosek bezpośredniego przełożonego, w nagłych sytuacjach, na wniosek bezpośredniego przełożonego- telefonicznie.
16) Login użytkownika, który utracił uprawnienia do przetwarzania danych nie może być przydzielony innej osobie.
17) Po otrzymaniu informacji o utracie przez użytkownika uprawnień do przetwarzania danych osobowych, IOD niezwłocznie dokonuje stosownej adnotacji w ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych, a Administrator odpowiedniego systemu informatycznego wyrejestrowuje osobę z systemu.
18) W uzasadnionych przypadkach przetwarzać dane osobowe w systemach informatycznych mogą na wniosek bezpośredniego przełożonego/ opiekuna praktykanci, stażyści, wolontariusze.
19) Bezpośredni przełożony/ opiekun praktykanta, stażysty, wolontariusza ponosi odpowiedzialność za zakres upoważnienia praktykanta, stażysty, wolontariusza w tym za wszystkie operacje wykonane w systemie informatycznym przez praktykanta, stażystę, wolontariusza.
20) Osoby przetwarzające dane osobowe są zobowiązane do zachowania ich w tajemnicy, a także sposobów ich zabezpieczenia, zarówno w trakcie zatrudnienia jak również po jego ustaniu.
21) Upoważnienia oraz oświadczenia, o których mowa powyżej sporządza się w 2 egzemplarzach (1 egzemplarz dla upoważnionego pracownika, 1 egzemplarz do akt osobowych).
22) IOD /LAS w ramach administrowanego systemu/ jest zobowiązany do prowadzenia ***Rejestru upoważnień*** do przetwarzania danych osobowych.
23) Administrator systemu przekazuje swoje hasło administratora (supervisora, roota, admina) do IOD, hasła powinny być przekazywane i przechowywane w opieczętowanej i opatrzonej podpisem administratora danego systemu informatycznego kopercie.

IOD zabezpiecza hasła w szafie pancernej, do której dostęp mają wyłącznie osoby uprawnione. IOD/ ASI może wykorzystać zdeponowane hasła tylko za zgodą AD, po komisyjnym dokonaniu otwarcia kopert z ich zawartością.

4. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu

1) Przystępując do pracy w systemie informatycznym, w którym przetwarzane są dane osobowe użytkownik wpisuje login oraz hasło dostępu w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione, a po uzyskaniu zatwierdzenia przez system uruchamia potrzebną aplikację.
2) Czas rozpoczynania i kończenia pracy w systemach informatycznych, w tym w systemach przetwarzających dane osobowe, jest zgodny z czasem pracy, obowiązującym danego pracownika. Pozostanie poza obowiązującym czasem pracy wymaga zgody kierownika/ koordynatora komórki organizacyjnej.
3) Krótkotrwałe przerwy w pracy (bez opuszczania stanowiska pracy) nie wymagają zamykania aplikacji.
4) Przed zakończeniem dnia pracy użytkownik powinien wylogować się z systemu oraz wyłączyć komputer.

5. *Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.*

1) Dane osobowe zabezpiecza się poprzez wykonywanie kopii zapasowych.
2) Ochronie poprzez wykonanie kopii podlegają także programy i narzędzia programowe służące przetwarzaniu danych. Kopie programów i narzędzi wykonywane są zaraz po instalacji oraz po każdej aktualizacji; na zewnętrznych, elektronicznych nośnikach informacji.
3) Zabezpieczeniu poprzez wykonywanie kopii zapasowych podlegają także dane konfiguracyjne systemu informatycznego przetwarzającego dane osobowe, w tym uprawnienia użytkowników systemu.
4) Za tworzenie kopii zapasowych odpowiada ASI.
5) Użytkownik tworzy wydruki związane z przetwarzaniem danych osobowych wyłącznie w zakresie i ilości niezbędnej dla celów służbowych w uzgodnieniu z bezpośrednim przełożonym.
6) Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia, należy zniszczyć w stopniu uniemożliwiającym ich odczytanie, a gdy jest to możliwe przy użyciu niszczarki dokumentów.

6. *Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych.*

1) Nośniki danych osobowych w postaci elektronicznej powinny być zabezpieczone przed dostępem osób nieuprawnionych, nieautoryzowaną modyfikacją i zniszczeniem.
2) Czas przechowywania kopii zapasowych zbiorów z serwerów ustala się na:

- kopia codzienna	- 3 dni
- kopia tygodniowa (piątkowa)	- 1 tydzień
- kopia miesięczna	- 1 miesiąc

- kopia roczna (nagrana na CD-ROM)- 5 lat, zmiana nośnika nie rzadziej niż co 2 lata.
3) Kopie zapasowe usuwa się niezwłocznie po ustaniu ich użyteczności.
4) Zniszczenia nośnika należy dokonać komisyjnie w obecności IOD i ASI lub wyznaczonego informatyka, w sposób adekwatny do określonego nośnika danych.

7. Sposób zabezpieczenia systemu informatycznego przed działalnością złośliwego oprogramowania

1) System informatyczny zabezpieczenia się programem antywirusowym przed działalnością złośliwego oprogramowania.
2) ASI jest odpowiedzialny za instalację i aktualizację tego programu.
3) System antywirusowy powinien być aktualizowany na podstawie materiałów publikowanych przez producenta oprogramowania.
4) W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy ASI podejmuje działania zmierzające do usunięcia zagrożenia za pomocą dostępnych narzędzi.
5) System informatyczny przetwarzający dane osobowe zabezpiecza się przed utratą danych w wyniku awarii zasilania przez podłączenie do zasilania awaryjnego.
6) We wszystkich komputerach w Szpitalu mogą być instalowane wyłącznie oprogramowania posiadające licencję.
7) Instalacji nowego oprogramowania dokonują wyłącznie Informatycy Szpitala lub zgodnie z umową dostawca specjalistycznego oprogramowania, w porozumieniu z ASI.
8) Użytkownikom systemu informatycznego zabrania się samowolnego instalowania jakiegokolwiek oprogramowania komputerowego.

8. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

1) Przeglądy i konserwacja urządzeń zawierających dane osobowe powinny być wykonywane w terminach określonych przez producenta sprzętu, lub zgodnie z potrzebami.
2) Prace serwisowe na terenie Szpitala mogą być wykonywane wyłącznie przez pracowników Szpitala (informatycy, pracownicy aparatury medycznej) lub przez upoważnionych przedstawicieli wykonawców zewnętrznych pracujących pod nadzorem pracowników Szpitala.
3) Przed rozpoczęciem prac serwisowych przez osoby spoza Szpitala konieczne jest potwierdzenie tożsamości serwisantów.

9. Procedura pracy zdalnej

1) Upoważnione przez administratora osoby mogą przetwarzać dane osobowe za pomocą zdalnego dostępu.
2) Wszystkie zdalne połączenia informatyków do sieci wewnętrznej Szpitala wymagają zgody Administratora lub ASI.
3) W wyjątkowych przypadkach, jeśli uzyskanie zgody od Administratora jest niemożliwe, dopuszcza się połączenie zdalne z systemem, informatyków Szpitala. Fakt ten łączący się informatyk zgłasza, najwcześniej jak jest to możliwe Administratorowi i IOD.
4) ASI prowadzi ***Rejestr zdalnych połączeń.***

10. Procedura dostępu podmiotów zewnętrznych do danych osobowych w systemach informatycznych

1) Podmioty zewnętrzne mogą otrzymać dostęp do systemów informatycznych Szpitala tylko jeżeli przewidują to zawarte z nimi umowy.
2) ASI nadzorujący realizację umowy z podmiotem zewnętrznym wnioskuje do Administratora o nadanie uprawnień dla pracowników podmiotu zewnętrznego.
3) Uprawnienia do systemów informatycznych dla pracowników podmiotu zewnętrznego są przyznawane nie dłużej niż na czas trwania umowy.
4) ASI zawsze jest informowany o potrzebie zdalnego dostępu, każdorazowo wydaje na nie zgodę oraz nadzoruje wykonywane prace.
5) IOD prowadzi rejestr upoważnionych podmiotów zewnętrznych, oraz użytkowników którym nadano uprawnienia do zdalnego dostępu do sieci informatycznej Szpitala.

11. Procedura korzystania ze służbowego komputera przenośnego

1) Pracownik zobowiązany jest zabezpieczyć dostęp do komputera w sposób uniemożliwiający zalogowanie się do systemu osobom nieuprawnionym.
2) Fakt utraty, uszkodzenia lub zniszczenia komputera należy niezwłocznie zgłosić bezpośredniemu przełożonemu.
3) Komputer przenośny nie może być pozostawiony bez właściwego zabezpieczenia /szafa zamykana na klucz/.
4) Komputer przenośny użytkowany poza siedzibą Szpitala musi być przechowywany w miejscach minimalizujących ryzyko przypadkowego uszkodzenia oraz kradzieży.
5) Komputery przenośne, które są użytkowane poza siedzibą Szpitala powinny być transportowane w specjalnie do tego celu przeznaczonych torbach, chroniących je przed uszkodzeniami mechanicznymi.

12. Procedura korzystania z Internetu

1) Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.
2) Zabrania się zgrywania na dysk twardy komputera oraz uruchamiania jakichkolwiek nielegalnych programów oraz plików.
3) Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.

13. Procedura korzystania z poczty elektronicznej

1) Przesyłanie danych osobowych z użyciem e- maila może odbywać się tylko jeśli został on zabezpieczony hasłem. Hasło należy przesłać odrębnym mailem lub inną drogą, np. telefonicznie lub SMS-em. W wyjątkowych sytuacjach drugim mailem.
2) W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne.
3) Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.

4) Pracownik powinien wykorzystywać służbową pocztę elektroniczną (służbowy adres e-mail) jedynie do czynności związanych z wykonywaną pracą.
5) Zabronione jest wykorzystywanie służbowej poczty elektronicznej (służbowego adresu e-mail) do celów prywatnych.
6) Zabronione jest wykorzystywanie prywatnej poczty elektronicznej (prywatnego adresu e-mail) do celów służbowych.

14. Zasady monitorowania przez pracodawcę: pracowników, sprzętu komputerowego i oprogramowania

1) Administrator ma prawo monitorować sposób wykonywania przez pracownika obowiązków wynikających ze stosunku pracy.
2) Nie jest dopuszczalne ukryte monitorowanie komputerów pracowników.
3) Kontrola jakościowa i ilościowa pracy przy komputerze może być wykonywana pod warunkiem poinformowania o tym pracownika.
4) Do realizacji czynności kontrolnych dopuszcza się monitoring za pomocą specjalistycznego oprogramowania.

ROZDZIAŁ VIII Wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe

1. Dane osobowe w Szpitalu przetwarza się w pomieszczeniach, w których Szpital prowadzi swoją działalność.
2. Przebywanie w pomieszczeniach, osób nieuprawnionych do dostępu do danych osobowych, jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych.
3. IOD prowadzi ***Wykaz pomieszczeń, w których przetwarzane są dane osobowe.***

ROZDZIAŁ IX Rejestr czynności przetwarzania danych osobowych

1. IOD prowadzi ***Rejestr czynności przetwarzania danych osobowych***.
2. Rejestr czynności przetwarzania danych osobowych zawiera:

1) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także IOD,
2) cele przetwarzania,
3) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych,
4) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione,
5) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,
6) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

3. Rejestr czynności przetwarzania danych osobowych zobowiązane są także prowadzić podmioty, którym Szpital powierzył przetwarzanie danych medycznych.

ROZDZIAŁ X Rejestr oceny skutków wpływu na prywatność

1. IOD w porozumieniu z ASI, przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji

przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

2. Nie dokonuje się oceny skutków, jeśli prawo reguluje daną operację. Jeżeli przetwarzanie reguluje daną operację przetwarzania lub zestaw operacji, a oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej (np. ustawy).

3. Ocenę skutków dla ochrony danych prowadzi się zgodnie z wykazem rodzajów operacji przetwarzania, ustanowionym przez organ nadzorczy.

4. Rejestr oceny skutków wpływu na prywatność powinien zawierać:

1) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania,

2) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów,

3) ocenę ryzyka naruszenia praw lub wolności osób fizycznych (pacjentów), których dane dotyczą,

4) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie unijnego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

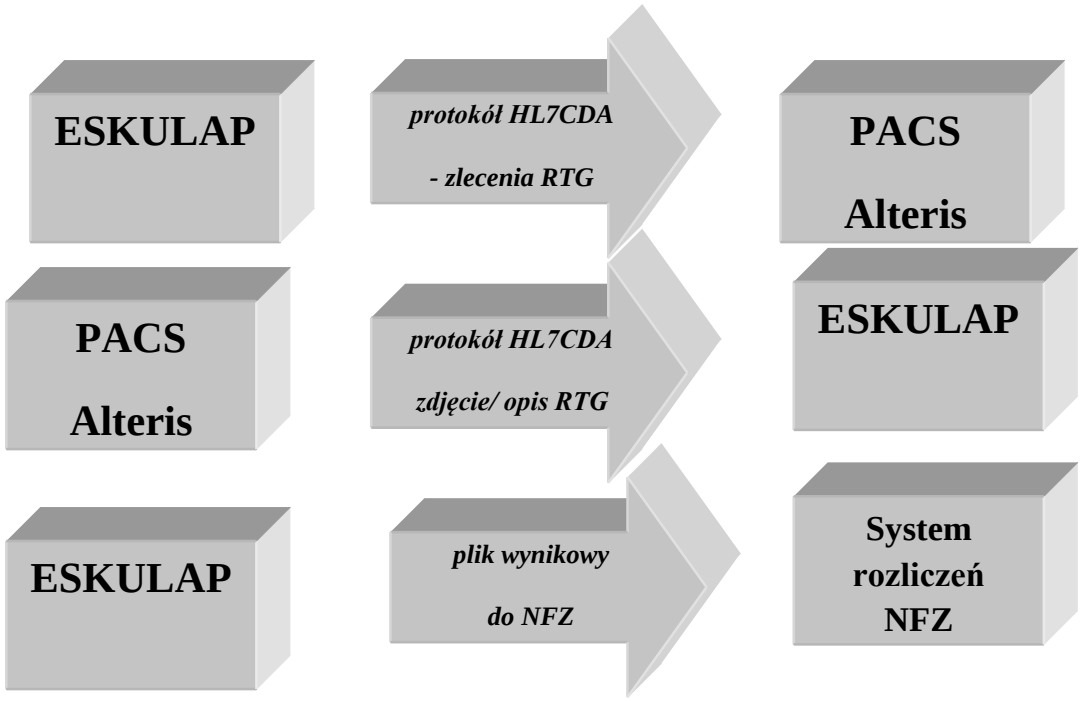
ROZDZIAŁ XI Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi znajduje się w bazie danego systemu.

ROZDZIAŁ XII Sposób przepływu danych pomiędzy poszczególnymi systemami

1. W większości powiązań pomiędzy systemami stosowane są protokoły HL7CDA, oraz zapytania i automaty do bazy sytemu.

2. W Szpitalu istnieją następujące schematy przepływu danych pomiędzy systemami w **części medycznej- białej:**



3. W Szpitalu istnieją następujące schematy przepływu danych pomiędzy systemami w **części administracyjnej- szarej:**

ROZDZIAŁ XIII Powierzenie przetwarzania danych osobowych

1. Szpital może powierzyć przetwarzanie danych innemu podmiotowi, na podstawie umowy lub innego instrumentu prawnego.
2. Umowa powierzenia przetwarzania danych powinna określać: przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą; prawa i obowiązki administratora oraz podmiotu przetwarzającego.
3. Podmiot przetwarzający:

1) przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora,
2) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
3) podejmuje wszelkie niezbędne środki bezpieczeństwa dla ochrony przetwarzanych danych,
4) przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o ile dysponuje szczegółową i pisemną zgodą administratora danych na dalsze powierzenie,
5) w miarę możliwości wspiera administratora w zakresie wywiązywania się przez niego z obowiązków związanych z ochroną danych osobowych, nałożonych treścią rozporządzenia, a także udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia powyższych obowiązków,
6) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo nakazuje przechowywanie danych osobowych,
7) umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji.

4. Podmiot zewnętrzny, któremu ma zostać powierzone przetwarzanie danych osobowych, jest zobowiązany przed rozpoczęciem przetwarzania danych do zapewnienia o stosowaniu

odpowiednich środków technicznych i organizacyjnych, by przetwarzanie chroniło prawa osób, których dane dotyczą.
5.IOD/ASI prowadzi ***Rejestr umów powierzenia przetwarzania danych osobowych.***

ROZDZIAŁ XIV Udostępnianie danych osobowych

1. Każda osoba ma prawo do dostępu do swoich danych (w tym do dokumentacji medycznej dotyczącej jego stanu zdrowia oraz udzielonych jej świadczeń zdrowotnych).
2. Udostępnienie danych osobowych następuje:
- na wniosek osoby, której dane dotyczą,
- na podstawie przepisów prawa,
- innemu administratorowi, jeżeli przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub stronę trzecią.
3. Fakt udostępnienia danych osobowych zawartych w dokumentacji medycznej oraz pozostałych danych osobowych należy odnotowywać w ***Rejestrze udostępnień dokumentacji z danymi osobowymi***; dostępny pod adresem: http://10.0.1.98

ROZDZIAŁ XV Archiwizowanie informacji zawierających dane osobowe

Okres archiwizacji dokumentów zawierających dane osobowe określa Jednolity Rzeczowy Wykaz Akt.

ROZDZIAŁ XVI Naruszenie ochrony danych osobowych

a) u administratora

1. Każdy pracownik ma obowiązek zgłosić wszelkie zdarzenia mogące naruszyć bezpieczeństwo danych osobowych, w tym urządzeń przetwarzających te dane.
2. Pracownik zgłaszający zdarzenie jest obowiązany podjąć działania mające na celu zminimalizowanie negatywnych skutków zaistniałego naruszenia oraz stosować się do zaleceń IOD i/lub ASI.
3. IOD oraz pracownik Zespołu ds. informatycznych/ASI dokonują wstępnej analizy czy naruszenie wpłynęło na bezpieczeństwo informacji u administratora, oraz zbierają materiał dowodowy (np. dokumenty papierowe, dokumenty elektroniczne, logi, pliki systemowe itp.).
4. Osoba, która odebrała zgłoszenie, powiadamia niezwłocznie Administratora danych o zaistniałym naruszeniu oraz sporządza notatkę o zaistniałym zdarzeniu.
5. Zgłoszeń dotyczących naruszeń bezpieczeństwa danych osobowych można dokonać:

a) drogą elektroniczną poprzez panel zgłaszania spraw (incydentów, naruszeń, usterek itp.), dostępny pod adresem: http://10.0.1.98;

b) telefonicznie do:

1) Inspektora Ochrony Danych (IOD) tel. 18 442 58 84; w dni robocze w godz. 7.30-15.05);
2) Zespołu ds. informatycznych/Administratora Systemu Informatycznego (ASI) tel. 18 442 59 73; w dni robocze w godz. 7.30-15.05;

3) poza godzinami pracy na numery telefonów podanych w Wykazie danych osobowych kadry kierowniczej oraz wyznaczonych pracowników upoważnionych do podejmowania działań w sprawach zarządzania kryzysowego w sytuacjach nadzwyczajnych (w szczególności nr tel. 795 531 805).

c) **e-mailowo** na adres:

- Inspektora Ochrony Danych (IOD): abi@szpitalnowysacz.pl)
- Zespołu ds. informatycznych: informatyka@szpitalnowysacz.pl
- sekretariatu Szpitala: sekretariat@szpitalnowysacz.pl; i/lub

d) **pisemnie** do Inspektora Ochrony Danych lub Koordynatora Zespołu ds. informatycznych, na adres Szpitala.

6. IOD prowadzi ***Rejestr naruszeń,*** w którym odnotowuje zaistniałe naruszenia.
7. Na podstawie analizy zaistniałych naruszeń IOD przedstawia administratorowi propozycje dodatkowych zabezpieczeń.

b) w podmiocie przetwarzającym

1. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi.
2. Zasady zgłaszania naruszeń, które wystąpiły w Podmiocie przetwarzającym, z którym Szpital ma podpisane umowy, zostają określone w Umowach powierzenia przetwarzania danych osobowych.
3. Po otrzymaniu informacji o naruszeniu w Podmiocie przetwarzającym, IOD dokonuje analizy jak w przypadkach zaistnienia naruszenia u administratora.

c) zgłaszanie naruszeń do organu nadzorczego

1. Administrator informuje organ nadzorczy - Urząd Ochrony Danych Osobowych- o każdym stwierdzonym naruszeniu zasad ochrony danych osobowych (chyba, że jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych).
2. Zgłoszenie naruszenia winno nastąpić w ciągu 72 godzin od jego stwierdzenia i musi co najmniej:
1) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
2) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych, od którego można uzyskać więcej informacji,
3) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,
4) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
3. IOD prowadzi ***Rejestr zgłoszeń naruszeń ochrony danych osobowych organowi nadzorczemu.***
4. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

ROZDZIAŁ XVII Przeglądy i aktualizacje Polityki

1. Polityka podlega przeglądowi pod kątem aktualności nie rzadziej niż raz do roku.
2. Przeglądu i aktualizacji Polityki dokonuje IOD. Polityka podlega aktualizacji każdorazowo w przypadku:
1) wdrożenia nowego systemu informatycznego,
2) zmiany przepisów prawa dotyczących ochrony danych osobowych, wymagających aktualizacji niniejszej Polityki,
3) innych znaczących zmian w funkcjonowaniu Szpitala mających wpływ na przetwarzanie danych osobowych.
3. IOD po uzgodnieniu z administratorem przeprowadza wewnętrzne kontrole zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Zakres, przebieg i rezultaty kontroli są dokumentowane i pisemnie przekazywane do administratora.

ROZDZIAŁ XVIII Postanowienia końcowe

1. **Polityka** jest dokumentem wewnętrznym i nie może być udostępniania osobom nieuprawnionym.
2. Kierownicy komórek organizacyjnych są zobowiązani zapoznać podległy personel z treścią **Polityki**.
3. Każda nowo zatrudniona osoba, upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się z **Polityką** przed dopuszczeniem jej do przetwarzania danych oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści.
4. ***Niezastosowanie się do prowadzonej przez administratora Polityki i naruszenie procedur ochrony danych przez pracowników, może być potraktowane jako ciężkie naruszenie podstawowych obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia z winy pracownika na podstawie art. 52 Kodeksu pracy.***
5. Niezależnie od rozwiązania stosunku pracy osoby popełniające przestępstwo będą pociągane do odpowiedzialności karnej.
6. W sprawach nieuregulowanych w **Polityce** mają zastosowanie przepisy ustawy o ochronie danych osobowych oraz wydane na jej podstawie akty wykonawcze.