Zarządzenie nr 28/2018
Dyrektora Wojewódzkiego Centrum Psychiatrii Długoterminowej
w Stroniu Śląskim SP ZOZ
z dnia 22 maja 2018 roku

w sprawie przyjęcia OCENY SKUTKÓW planowanych operacji oraz PLANU POSTĘPOWANIA z RYZYKIEM dla ochrony danych osobowych w Wojewódzkim Centrum Psychiatrii Długoterminowej w Stroniu Śląskim SP ZOZ.

Na podstawie § 5 pkt 1, § 6 ust. 1 Statutu Wojewódzkiego Centrum Psychiatrii Długoterminowej- załącznik do uchwały Sejmiku Województwa Dolnośląskiego z dnia 20 grudnia 2012 r., nr XXX/839/12 w związku z § 35 rozporządzania Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zarządza się, co następuje:

§1.
OCENA SKUTKÓW planowanych operacji dla ochrony danych osobowych (DPIA) w Wojewódzkim Centrum Psychiatrii Długoterminowej w Stroniu Śląskim SP ZOZ.

Ilekroć w OCENIE jest mowa o:

1) Jednostce- należy przez to rozumieć Wojewódzkie Centrum Psychiatrii Długoterminowej w Stroniu Śląskim SP ZOZ,
2) Danych osobowych- należy przez to rozumieć zbiór/zbiory danych osobowych dotyczące zdrowia fizycznego lub psychicznego pacjentów i pracowników Jednostki,
3) Pacjencie- należy przez to rozumieć osobę zwracającą się o udzielenie świadczeń zdrowotnych lub korzystającą ze świadczeń zdrowotnych udzielanych przez Jednostkę,
4) Operacjach przetwarzania- należy przez to rozumieć operacja polegające w szczególności na zbieraniu, utrwalaniu, porządkowaniu, przechowywaniu, adaptowaniu, modyfikowaniu, pobieraniu, przeglądaniu, usuwaniu, niszczeniu.
5) Odbiorcy- należy przez to rozumieć osobę fizyczną lub prawną, której ujawnia się dane osobowe zgromadzone w Jednostce,
6) Podmiocie przetwarzającym dane (procesorze)- należy przez to rozumieć osobę fizyczną lub osobę prawną, która przetwarza dane osobowe w imieniu Jednostki, na podstawie stosownej umowy zawartej pomiędzy stronami,
7) Organie Nadzorczym- należy przez to rozumieć Prezesa Urzędu Ochrony Danych Osobowych.

§2
Opis planowanych operacji przetwarzania danych osobowych i celów przetwarzania.

1. Celem przetwarzania danych osobowych w Jednostce jest realizowanie przez Jednostkę prawnie uzasadnionych interesów, w tym w szczególności:
1) konieczność świadczenia usług medycznych,
2) wykonywanie innych obowiązków z zakresu ochrony zdrowia,
3) leczenie Pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych,
4) zarządzanie udzielaniem usług medycznych;

w tym także prawidłowe wykonywanie obowiązków, nałożonych na Jednostkę w szczególności przez ustawy:

5) z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2017 r., poz. 1318),
6) z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego (Dz. U. z 2017 r., poz. 882),
7) z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz. U. z 2018 r., poz. 160),
8) z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowych ze środków publicznych (Dz. U. z 2017 r., poz. 1938),
9) z dnia 5 grudnia 1996 r. o zawadach lekarza i lekarza dentysty (Dz. U. z 2018 r., poz. 617),
10) z dnia 15 lipca 2011 r. o zawodach pielęgniarki i położnej (Dz. U. z 2018 r., poz. 123).

§3.

W Jednostce wykonuje się stale operacje przetwarzania danych osobowych, związanych w szczególności z:
1) świadczeniu usług opieki zdrowotnej oraz zarządzaniu systemami i usługami opieki zdrowotnej, w tym w szczególności:
a) rejestracji pacjentów,
b) przyjęciu pacjentów do Jednostki,
c) przypominaniu o terminie realizacji świadczenia,
d) odbieraniu i archiwizowaniu oświadczeń woli pacjentów,
e) weryfikacji uprawnień i rozliczanie świadczeń,
f) utrzymaniu systemu teleinformatycznego,
g) wymianie informacji pomiędzy systemem Jednostki, a innymi podmiotami w celu zapewnienia ciągłości opieki,
h) wystawianiu zaświadczeń lekarskich
2) zarządzaniu jednostką, w tym w szczególności:
a) rekrutacji pracowników;
b) prowadzeniu rejestru pracowników, akt pracowniczych i ewidencji czasu ich pracy;
c) zgłoszeniu pracowników i członków ich rodzin do ZUS,
d) aktualizacji zgłoszeń i przekazywanie danych o zwolnieniach;
d) prowadzeniu rozliczeń z pracownikami,
e) wypłacie wynagrodzeń,
f) naliczaniu obciążeń oraz naliczanie składek do ZUS.

§4.

Podczas przetwarzania danych osobowych w Jednostce:
1) zapewniony jest systematyczny opis planowanych operacji przetwarzania danych,
2) uwzględniony jest charakter, zakres, kontekst i cele przetwarzania danych,
3) dokumentowane są dane osobowe Odbiorcy danych,
4) uwzględnia się okres przechowywania danych,
5) funkcjonuje opis operacji przetwarzania danych,
6) zidentyfikowane są aktywa, na których opierają się dane tj.:
a) sprzęt- wszelkie urządzenia fizyczne w organizacji tj.: urządzenia przenośne, stacjonarne, peryferyjne, nośniki danych,
b) oprogramowanie- wszelkie programy uczestniczące w operacjach przetwarzania danych,
c) sieci- wszystkie urządzenia telekomunikacyjne używane do połączenia wielu fizycznie oddalonych komputerów lub elementów systemu informacyjnego,
d) ludzie/personel- wszystkie osoby zaangażowane w przetwarzania danych,

e) dokumenty papierowe lub papierowe kanały transmisji,
f) siedziba- wszelkie lokalizacje wykorzystywane do przetwarzania danych.
7) uwzględnia się zgodność przetwarzania danych z zatwierdzonymi kodeksami postępowania.
8) uwzględnia się okres przechowywania danych.

§5.
Ocena, czy operacje przetwarzania są niezbędne oraz proporcjonalne do oczekiwanych celów

1. Wykonywane w Jednostce operacje przetwarzania danych osobowych, są niezbędne oraz proporcjonalne dla osiągnięcia zakładanych celów określonych w § 3 niniejszej OCENY.
2. Przed przystąpieniem do wykonywania operacji przetwarzania danych osobowych, ustala się niezbędność oraz proporcjonalność każdej z planowanych operacji przetwarzania, w oparciu o:
1) konkretny, wyraźny i prawnie uzasadniony cel(e) przetwarzania,
2) zgodność przetwarzania z prawem,
3) ustalenie czy dane osobowe są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, dla których są przetwarzane,
4) ograniczony czas przechowywania danych,
5) konieczność zapewnienia odpowiednich środków technicznych, w celu przekazania osobie, której dane dotyczą, wszelkich informacji wymaganych prawem,
6) ograniczenie liczby Odbiorców danych,
7) ograniczenie liczby Podmiotów przetwarzających dane,
8) uprzednie konsultacje z Organem Nadzorczym.

§6.
Ocena ryzyka naruszenia praw i wolności osób fizycznych, których dane dotyczą (szacowanie ryzyka)

1. Z dużym prawdopodobieństwem ocenia się, że dane osobowe, które podlegają operacjom przetwarzania w Jednostce, są w małym stopniu narażane na naruszenie. Niniejsze naruszenia danych osobowych możemy podzielić na:
1) Zagrożenia losowe zewnętrzne, które mogą polegać w szczególności na:
a) wystąpieniu klęsk żywiołowych,
b) wybuchu gazu, pożarze, zalaniu.
c) działaniach terrorystycznych,
d) nieprawidłowościach w zakresie zabezpieczenia fizycznego miejsc przechowywania i przetwarzania danych osobowych.

2) Zagrożenia losowe wewnętrzne, które mogą polegać w szczególności na:
a) pomyłkach Administratora danych,
b) pomyłkach Inspektora Ochrony Danych Osobowych,
c) awarii sprzętu,
d) błędach oprogramowania.

3) Zagrożenia zamierzone, które mogą polegać w szczególności na:
a) nieuprawnionym dostępie do systemu z zewnątrz (włamanie)
b) nieuprawnionym dostępie do systemu z jego wnętrza,
c) nieuprawnionym przekazaniu danych osobowych,
d) bezpośrednim zagrożeniu materialnych składników (kradzież)

2. Ocena ryzyka naruszenia danych, została dokonana w oparciu o:
1) kontekst przetwarzania danych osobowych,
2) odpowiednie szacowanie ryzyka,
3) akceptację ryzyk cząstkowych.

§7.

Graficzne przedstawienie OCENY SKUTKÓW planowanych operacji oraz PLANU POSTĘPOWANIA z RYZYKIEM dla ochrony danych osobowych w Wojewódzkim Centrum Psychiatrii Długoterminowej w Stroniu Śląskim SP ZOZ, zawiera załącznik nr 1 do niniejszego zarządzenia.

§8.

PLAN POSTĘPOWANIA z RYZYKIEM - Planowane środki w celu zaradzenia ryzyku, mające zapewnić ochronę danych osobowych oraz środki w celu przestrzegania rozporządzania Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (zarządzenie ryzykiem) w Wojewódzkim Centrum Psychiatrii Długoterminowej w Stroniu Śląskim SP ZOZ.

1. W celu zminimalizowania ewentualnych naruszeń danych osobowych i wystąpienia ryzyka w Jednostce, dokonuje się wyboru wariantu postępowania z ryzykiem oraz planuje się odpowiednie zabezpieczenia organizacyjne i techniczne, mających zapewnić ochronę danych osobowych i wykazać zgodność z obowiązującym prawem, z uwzględnieniem praw i prawnie uzasadnionych interesów osób fizycznych, których dane dotyczą, i innych osób fizycznych, których sprawa dotyczy, zapewniające:
1) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
2) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
3) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.
2. Środki, o którym mowa w ust. 1, polegają w szczególności na:
1) wprowadzeniu zabezpieczeń fizycznych, tj.:
a) zabezpieczeniu pomieszczeń drzwiami zwykłymi, wzmacnianymi i antywłamaniowymi,
b) zabezpieczenie w postaci zastosowania systemu alarmowego przeciwwłamaniowego(budynek archiwum),
c) zastosowanie systemu monitoringu, czyli kamery przemysłowe, lub też nadzór pomieszczeń przez portierów,
d) zabezpieczenie pomieszczenia przed skutkami pożaru za pomocą systemu przeciwpożarowego i wolno stojących gaśnic,
e) przechowywanie kopii zapasowych/archiwalnych zbioru danych osobowych w zamkniętej niemetalowej szafie lub w sejfie,

2) wprowadzeniu środków sprzętowej infrastruktury informatycznej i telekomunikacyjnej, polegających na:
a) zastosowaniu oprogramowania antywirusowego, stale aktualizowanego,
b) zabezpieczeniu dostępu do systemu operacyjnego komputera, na którym przetwarzane są dane osobowe za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,
c) przyjęcie mechanizmu wymuszającego okresową zmianę haseł w aplikacjach przetwarzających dane,
d) zastosowaniu urządzenia typu UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania,
e) zastosowaniu odrębnego zasilania sprzętu komputerowego oraz zastosowanie zasilania awaryjnego.
f) zastosowanie ograniczonego dostępu do pomieszczeń, w których następuje przetwarzanie danych osobowych (wyłączny dostęp osób bezpośrednio związanych z wykonywaniem nadzoru nad serwerami lub aplikacjami).

3) wprowadzeniu środków ochrony w ramach narzędzi programowych i baz danych, tj.:

a) wprowadzeniu środków umożliwiających rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych,

b) wprowadzenie systemu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła lub wykorzystaniem technologii biometrycznej,

c) wprowadzeniu środków umożliwiających określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych,

d) wprowadzenie kryptograficznych środków ochrony danych osobowych,

e) zainstalowanie wygaszaczy ekranów na stanowiskach, na których przetwarzane są dane osobowe,

g) wprowadzenie mechanizmu automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

4) wprowadzeniu środków organizacyjnych, tj.:

a) odpowiednim przeszkoleniu osób, które zostały zatrudnione przy nieprzetwarzaniu danych osobowych w zakresie ochrony danych osobowych,

b) odpowiednie ustawienie monitorów komputerów, na których przetwarzane są dane osobowe by uniemożliwiało wgląd osobom postronnym w przetwarzane dane,

c) niszczeniu dokumentów papierowych, zawierające dane osobowe po ustaniu ich przydatności,

d) odpowiednim zabezpieczeniu dokumentów zawierających dane osobowe, przez ich zamykanie w biurkach lub w przeznaczonych do tego szafach metalowych, niemetalowych lub w kasie pancernej.

§9.

Zarządzenie wchodzi w życie z dniem podpisania, z mocą obowiązującą od dnia 25 maja 2018 r.

§10.

Graficzne przedstawienie OCENY SKUTKÓW planowanych operacji oraz PLAN POSTĘPOWANIA z RYZYKIEM, a także ARKUSZ ZARZĄDZANIA RYZYKIEM dla ochrony danych osobowych w Wojewódzkim Centrum Psychiatrii Długoterminowej w Stroniu Śląskim SP ZOZ, zawiera załącznik nr 1 i 2 do niniejszego zarządzenia.

DYREKTOR CENTRUM
Joanna Chromiec

GŁÓWNY SPECJALISTA
ds. obsługi prawnej
mgr Sebastian Łukasiewicz

PROCES OCENY SKUTKÓW DLA OCHRONY DANYCH (DPIA)					
Analiza ryzyka przetwarzania					
Działania w zakresie zarządzania ryzykiem naruszenia praw i wolności osób, których dane dotyczą (art. 35 ust. 7 lit. c RODO)					
l.p.	**Kategoria Aktywów**	**Źródło Ryzyka (zagrożenia)**	**Zdarzenia (Ryzyka)**	**Wpływ zdarzenia na atrybuty:** **- poufności** **- integralności** **- dostępności**	**Identyfikacja skutków zdarzenia**
	Aktywa- rozumiane jako środki umożliwiające dokonywanie przetwarzania danych osobowych dla danej czynności (procesu).	Źródła ryzyka jako potencjalne sytuacje, jakie mogą powstać w aktywach w odniesieniu do danego procesu.	Wskazanie, jakie negatywne zdarzenia/sytuacje mogą powstać w przypadku zmaterializowania się źródła ryzyka.	**Naruszenie poufności-** nieuprawnione lub przypadkowe ujawnienie bądź udostępnienie danych. **Naruszenie integralności-** wprowadzenie nieuprawnionych zmian podczas odczytu/zapisu/transmisji/ modyfikacji/przechowywania. **Naruszenie dostępności-** brak możliwości wykorzystania danych na żądanie, w założonym czasie przez osobę uprawnioną.	Należny wskazać jakie zdarzenia powodujące naruszenie praw lub wolności osób fizycznych mogą mieć potencjalne skutki dla tych osób, których dane są przetwarzane w procesie.
1.	Dokumenty papierowe takie jak: - dokumentacja medyczna pensjonariuszy (pacjentów) - dane identyfikacyjne kuratorów i opiekunów w tym miejsca zamieszkania, - rejestr wybrakowanej dokumentacji medycznej,	- modyfikacja, - nieprawidłowe użytkowanie, - podglądanie/ podsłuchiwanie, -przepracowanie/ nadmierny stres/niestosowanie wewnętrznych	- nieuprawniony dostęp do danych osobowych, - niepożądane zmiany danych osobowych, -niezapisanie danych osobowych, - ujawnienie danych osobowych, - utrata danych osobowych.	P I D	- błąd przy wprowadzaniu danych, - błędna interpretacja i zastosowanie przepisów o ochronie danych osobowych, - błędna weryfikacja posiadanych danych osobowych, - celowa modyfikacja danych, - kradzież danych przez pracowników, - nadużycia pracowników prowadzące do naruszenia ochrony danych osobowych,

	- decyzje ZUS, Urzędów Pomocy Społecznej, Urzędów Pracy w sprawie przyznanych świadczeń pensjonariuszom (pacjentom), -inna dokumentacja dotycząca pensjonariuszy (pacjentów) w tym w szczególności: lista pacjentów korzystających z wyjazdów wycieczkowych, rejestr spadkobierców pacjentów, rejestr imienny pacjentów, rejestr spadkobierców pacjentów, rejestr korespondencji i paczek, - dokumentacja archiwalna(archiwum)- pacjentów, w tym spisy zdawczo-odbiorcze w archiwum, a także rejestr wypożyczeń dokumentacji medycznej. - dokumentacja pracowników i zleceniobiorców taka jak imię i nazwisko pracownika lub zleceniobiorcy lub osoby prowadzącej jednoosobową działalność gospodarczą lub spółkę cywilną, dane adresowe, nr PESEL, nr NIP, nr REGON, wykształcenie, zakres prowadzonej działalności gospodarczej, dane o poprzednim zatrudnieniu (staż pracy), dane o przyznanych karach, nagrodach i potrąceniach, zajęciach komorniczych, dane o absencji (urlopy okolicznościowe, urlopy wypoczynkowe, choroby, rehabilitacja itp.),	procedur/działanie wrogie pracowników, - utrata, - zniszczenie.			- nieobsłużenie naruszenia ochrony danych osobowych w ustawowym terminie, - nieświadome naruszenie ochrony danych osobowych przez pracowników wskutek błędu, - nieterminowa obsługa zgłoszeń dotyczących danych osobowych (np. zgłoszeń dotyczących praw osób, których dane dotyczą), - zagubienie dokumentów papierowych, - zmiana treści żądania, - zmiana sekwencji danych prowadząca do ryzyka nieprawidłowego zaadresowania/skierowania komunikatu/wpisania wyników pacjenta, - pomyłka przy rejestracji, - pomyła przy wpisaniu wyników pacjenta, - pomyła przy wysyłce danych pacjenta, - pomyła przy weryfikacja tożsamości pacjenta, - przesłanie danych osobowych do osoby/podmiotu nieuprawnionego.

	dane niezbędne w celu wypłaty świadczeń z ZFŚS oraz prowadzenia Pracowniczej Kasy Zapomogowo Pożyczkowej, dane o niepełnosprawności, dane o otrzymywanym wynagrodzeniu , - inna dokumentacja dotycząca pracowników w tym rejestr wydanej odzieży ochronnej i środków ochrony indywidualnej, rejestr wypadków (w tym protokoły powypadkowe, rejestr zakłuć), karty zasiłkowe, karty zarobkowe, informacje o zarobkach rocznych PIT- y, ewidencja akt osobowych, lista plac,deklaracje ubezpieczeniowe pracowników (dokumentacja ubezpieczeniowa), rejestr delegacji służbowych, ewidencja osób upoważnionych do przetwarzania danych osobowych, rejestr delegacji służbowych, - dokumentacja archiwalna (archiwum)- pracowników i zleceniobiorców, w tym spisy zdawczo-odbiorcze w archiwum. - dokumentacja z postępowań sądowych. Rejestr zawartych umów cywilnoprawnych.				
2.	Programy takie jak: - InfoMedica (kadry i płace, izba przyjęć i oddział i apteka),	- modyfikacja programu, - nieprawidłowe użycie oprogramowania, - nieprawidłowe	- nieuprawniony dostęp do danych osobowych, - niepożądane zmiany danych osobowych, -niezapisanie	P I D	- błąd przy wprowadzaniu danych, - błędna interpretacja i zastosowanie przepisów o ochronie danych osobowych, - błędna weryfikacja posiadanych danych

	- Płatnik, - program finansowo księgowy- Asseco.	użytkowanie, - podglądanie/ podsłuchiwanie, - przeciążenie, -przepracowanie/ nadmierny stres/niestosowanie wewnętrznych procedur/działanie wrogie pracowników, - utrata kontroli nad oprogramowaniem, - zniszczenie danych/systemów przetwarzających dane.	danych osobowych, - ujawnienie danych osobowych, - utrata danych osobowych.		osobowych, - błędna dane w systemach identyfikujące pensjonariusza (pacjenta), - celowa modyfikacja danych, - kradzież danych przez pracowników, - nadużycia pracowników prowadzące do naruszenia ochrony danych osobowych, - nieobsłużenie naruszenia ochrony danych osobowych w ustawowym terminie, - nieświadome naruszenie ochrony danych osobowych przez pracowników wskutek błędu, - nieterminowa obsługa zgłoszeń dotyczących danych osobowych (np. zgłoszeń dotyczących praw osób, których dane dotyczą), - ryzyko kradzieży sprzętu komputerowego, nośników, dokumentów przez pracowników lub osoby trzecie, - trudności w usunięciu danych konkretnej osoby ze wszystkich zasobów teleinformatycznych, - zbyt mała pojemność dysku, - zbyt duża liczna rekordów/danych o pacjentach powodująca przeładowanie systemu, - zmiana treści żądania, - zmiana sekwencji danych prowadząca do ryzyka nieprawidłowego zaadresowania/skierowania komunikatu/wpisania wyników pacjenta, - pomyłka przy rejestracji, - pomyła przy wpisaniu wyników pacjenta, - pomyła przy wysyłce danych pacjenta, - pomyła przy weryfikacja tożsamości pacjenta, - przesłanie danych osobowych do osoby/podmiotu nieuprawnionego, - wstrzymanie wykonywania praw osób fizycznych w wyniku przerwania usług IT.
3.	Personel	- podglądanie/ podsłuchiwanie, - przeciążenie, -przepracowanie/ nadmierny stres/niestosowanie	- nieuprawniony dostęp do danych osobowych, - niepożądane zmiany danych osobowych, -niezapisanie danych osobowych,	P I D	- błąd przy wprowadzaniu danych, - błędna interpretacja i zastosowanie przepisów o ochronie danych osobowych, - błędna weryfikacja posiadanych danych osobowych, - błędna dane w systemach identyfikujące

		wewnętrznych procedur/działanie wrogie pracowników.	- ujawnienie danych osobowych, - utrata danych osobowych.		pensjonariusza (pacjenta), - celowa modyfikacja danych, - kradzież danych przez pracowników, - nadużycia pracowników prowadzące do naruszenia ochrony danych osobowych, - nieobsłużenie naruszenia ochrony danych osobowych w ustawowym terminie, - nieświadome naruszenie ochrony danych osobowych przez pracowników wskutek błędu, - nieterminowa obsługa zgłoszeń dotyczących danych osobowych (np. zgłoszeń dotyczących praw osób, których dane dotyczą), - ryzyko kradzieży sprzętu komputerowego, nośników, dokumentów przez pracowników lub osoby trzecie, - trudności w usunięciu danych konkretnej osoby ze wszystkich zasobów teleinformatycznych, - zbyt mała pojemność dysku, - zbyt duża liczna rekordów/danych o pacjentach powodująca przeładowanie systemu, - zagubienie dokumentów papierowych, - zmiana treści żądania, - zmiana sekwencji danych prowadząca do ryzyka nieprawidłowego zaadresowania/skierowania komunikatu/wpisania wyników pacjenta, - pomyłka przy rejestracji, - pomyła przy wpisaniu wyników pacjenta, - pomyła przy wysyłce danych pacjenta, - pomyła przy weryfikacja tożsamości pacjenta, - przesłanie danych osobowych do osoby/podmiotu nieuprawnionego, - wstrzymanie wykonywania praw osób fizycznych w wyniku przerwania usług IT.
4.	Przesyłanie dokumentów	- modyfikacja, - nieprawidłowe użycie oprogramowania, - nieprawidłowe użytkowanie, - podglądanie/ podsłuchiwanie,	- nieuprawniony dostęp do danych osobowych, - niepożądane zmiany danych osobowych, -niezapisanie danych osobowych, - ujawnienie danych	P I D	- błąd przy wprowadzaniu danych, - błędna interpretacja i zastosowanie przepisów o ochronie danych osobowych, - błędna weryfikacja posiadanych danych osobowych, - błędna dane w systemach identyfikujące pensjonariusza (pacjenta),

		- przeciążenie, -przepracowanie/ nadmierny stres/niestosowanie wewnętrznych procedur/działanie wrogie pracowników, - utrata kontroli nad oprogramowaniem, - zniszczenie danych/systemów przetwarzających dane.	osobowych, - utrata danych osobowych.		- celowa modyfikacja danych, - kradzież danych przez pracowników, - nadużycia pracowników prowadzące do naruszenia ochrony danych osobowych, - nieobsłużenie naruszenia ochrony danych osobowych w ustawowym terminie, - nieświadome naruszenie ochrony danych osobowych przez pracowników wskutek błędu, - nieterminowa obsługa zgłoszeń dotyczących danych osobowych (np. zgłoszeń dotyczących praw osób, których dane dotyczą), - ryzyko kradzieży sprzętu komputerowego, nośników, dokumentów przez pracowników lub osoby trzecie, - trudności w usunięciu danych konkretnej osoby ze wszystkich zasobów teleinformatycznych, - zbyt mała pojemność dysku, - zbyt duża liczna rekordów/danych o pacjentach powodująca przeładowanie systemu, - zagubienie dokumentów papierowych, - zmiana treści żądania, - zmiana sekwencji danych prowadząca do ryzyka nieprawidłowego zaadresowania/skierowania komunikatu/wpisania wyników pacjenta, - pomyłka przy rejestracji, - pomyła przy wpisaniu wyników pacjenta, - pomyła przy wysyłce danych pacjenta, - pomyła przy weryfikacja tożsamości pacjenta, - przesłanie danych osobowych do osoby/podmiotu nieuprawnionego, - wstrzymanie wykonywania praw osób fizycznych w wyniku przerwania usług IT.
5.	Siec (podłączenia komputerowe)	- przeciążenie, -przepracowanie/ nadmierny stres/niestosowanie wewnętrznych procedur/działanie wrogie pracowników, - utrata kontroli nad	- nieuprawniony dostęp do danych osobowych, - niepożądane zmiany danych osobowych, -niezapisanie danych osobowych, - ujawnienie danych osobowych,	P I D	- błąd przy wprowadzaniu danych, - błędna interpretacja i zastosowanie przepisów o ochronie danych osobowych, - błędna weryfikacja posiadanych danych osobowych, - błędna dane w systemach identyfikujące pensjonariusza (pacjenta), - celowa modyfikacja danych,

		oprogramowaniem, - zniszczenie danych/systemów przetwarzających dane.	- utrata danych osobowych.		- kradzież danych przez pracowników, - nadużycia pracowników prowadzące do naruszenia ochrony danych osobowych, - nieobsłużenie naruszenia ochrony danych osobowych w ustawowym terminie, - nieświadome naruszenie ochrony danych osobowych przez pracowników wskutek błędu, - nieterminowa obsługa zgłoszeń dotyczących danych osobowych (np. zgłoszeń dotyczących praw osób, których dane dotyczą), - ryzyko kradzieży sprzętu komputerowego, nośników, dokumentów przez pracowników lub osoby trzecie, - trudności w usunięciu danych konkretnej osoby ze wszystkich zasobów teleinformatycznych, - zbyt mała pojemność dysku, - zbyt duża liczna rekordów/danych o pacjentach powodująca przeładowanie systemu, - zagubienie dokumentów papierowych, - zmiana treści żądania, - zmiana sekwencji danych prowadząca do ryzyka nieprawidłowego zaadresowania/skierowania komunikatu/wpisania wyników pacjenta, - pomyłka przy rejestracji, - pomyła przy wpisaniu wyników pacjenta, - pomyła przy wysyłce danych pacjenta, - pomyła przy weryfikacja tożsamości pacjenta, - przesłanie danych osobowych do osoby/podmiotu nieuprawnionego, - wstrzymanie wykonywania praw osób fizycznych w wyniku przerwania usług IT.
6.	Siedziba przetwarzania	- zniszczenie, - nieprawidłowe użytkowanie (instalacji elektrycznej, gazowej, wind itp.), - podglądanie/ podsłuchiwanie, -przepracowanie/ nadmierny	- nieuprawniony dostęp do danych osobowych, - niepożądane zmiany danych osobowych, -niezapisanie danych osobowych, - ujawnienie danych osobowych, - utrata danych osobowych.	P I D	- błąd przy wprowadzaniu danych, - błędna interpretacja i zastosowanie przepisów o ochronie danych osobowych, - błędna weryfikacja posiadanych danych osobowych, - błędna dane w systemach identyfikujące pensjonariusza (pacjenta), - celowa modyfikacja danych, - kradzież danych przez pracowników,

		stres/niestosowanie wewnętrznych procedur/działanie wrogie pracowników.			- nadużycia pracowników prowadzące do naruszenia ochrony danych osobowych, - nieobsłużenie naruszenia ochrony danych osobowych w ustawowym terminie, - nieświadome naruszenie ochrony danych osobowych przez pracowników wskutek błędu, - nieterminowa obsługa zgłoszeń dotyczących danych osobowych (np. zgłoszeń dotyczących praw osób, których dane dotyczą), - ryzyko kradzieży sprzętu komputerowego, nośników, dokumentów przez pracowników lub osoby trzecie, - trudności w usunięciu danych konkretnej osoby ze wszystkich zasobów teleinformatycznych, - zbyt mała pojemność dysku, - zbyt duża liczna rekordów/danych o pacjentach powodująca przeładowanie systemu, - zagubienie dokumentów papierowych, - zmiana treści żądania, - zmiana sekwencji danych prowadząca do ryzyka nieprawidłowego zaadresowania/skierowania komunikatu/wpisania wyników pacjenta, - pomyłka przy rejestracji, - pomyła przy wpisaniu wyników pacjenta, - pomyła przy wysyłce danych pacjenta, - pomyła przy weryfikacja tożsamości pacjenta, - przesłanie danych osobowych do osoby/podmiotu nieuprawnionego, - wstrzymanie wykonywania praw osób fizycznych w wyniku przerwania usług IT.
7.	Sprzęt komputerowy	- samoczynna awaria, - samoczynne zniszczenie, - modyfikacja, - nieprawidłowe użytkowanie, - podglądanie/ podsłuchiwanie, -przepracowanie/ nadmierny	- nieuprawniony dostęp do danych osobowych, - niepożądane zmiany danych osobowych, -niezapisanie danych osobowych, - ujawnienie danych osobowych, - utrata danych osobowych.	P I D	- błąd przy wprowadzaniu danych, - błędna interpretacja i zastosowanie przepisów o ochronie danych osobowych, - błędna weryfikacja posiadanych danych osobowych, - błędna dane w systemach identyfikujące pensjonariusza (pacjenta), - celowa modyfikacja danych, - kradzież danych przez pracowników, - nadużycia pracowników prowadzące do naruszenia

		stres/niestosowanie wewnętrznych procedur/działanie wrogie pracowników, - utrata, - zniszczenie.			ochrony danych osobowych, - nieobsłużenie naruszenia ochrony danych osobowych w ustawowym terminie, - nieświadome naruszenie ochrony danych osobowych przez pracowników wskutek błędu, - nieterminowa obsługa zgłoszeń dotyczących danych osobowych (np. zgłoszeń dotyczących praw osób, których dane dotyczą), - ryzyko kradzieży sprzętu komputerowego, nośników, dokumentów przez pracowników lub osoby trzecie, - trudności w usunięciu danych konkretnej osoby ze wszystkich zasobów teleinformatycznych, - zbyt mała pojemność dysku, - zbyt duża liczna rekordów/danych o pacjentach powodująca przeładowanie systemu, - zagubienie dokumentów papierowych, - zmiana treści żądania, - zmiana sekwencji danych prowadząca do ryzyka nieprawidłowego zaadresowania/skierowania komunikatu/wpisania wyników pacjenta, - pomyłka przy rejestracji, - pomyła przy wpisaniu wyników pacjenta, - pomyła przy wysyłce danych pacjenta, - pomyła przy weryfikacja tożsamości pacjenta, - przesłanie danych osobowych do osoby/podmiotu nieuprawnionego, - wstrzymanie wykonywania praw osób fizycznych w wyniku przerwania usług IT.

OCENA RYZYKA

Prawdopodobieństwo zdarzenia		**Konsekwencja zdarzenia dla osoby fizycznej**		**Ocena ryzyka**
Poziom (1-4)	**Uzasadnienie wyboru wartości**	**Poziom (1-4)**	**Uzasadnienie wyboru wartości**	**Poziom ryzyka**
1	(1)- **mało prawdopodobne.** Raczej nie zdarzy się w ciągu roku, bądź prawdopodobieństwo jest mniejsze niż od 10%. (2)- **możliwe.** Raczej zdarzy się w ciągu roku, bądź	1	(1)- **ograniczone naruszenie**- osoba, której dane dotyczą, nie odczuje wpływu lub zetknie się z niewielką liczbą niedogodności, które łatwo może pokonać/naprawić. (2)- **naruszenie**- osoba, której dane dotyczą, może napotkać znaczące niedogodności, które będzie wstanie pokonać/naprawić przy nakładzie czasu i wysiłku.	**M**- małe
2		2		**Ś**- średnie
3		3		**W**- wysokie
4		4		**BW**- bardzo wysokie

	prawdopodobieństwo zdarzenia wynosi powyżej 10% , ale poniżej 25%. (3)- **prawdopodobne.** Raczej zdarzy się w ciągu miesiąca, bądź prawdopodobieństwo zdarzenia wynosi powyżej 25% , ale poniżej 50%. (4)- **wysokie prawdopodobieństwa lub pewność wystąpienia.** Raczej zdarzy się w ciągu miesiąca, bądź prawdopodobieństwo zdarzenia wynosi powyżej 50%.		(3)- **znaczące naruszenie**- osoba, której dane dotyczą, może napotkać znaczące konsekwencje, które powinna móc pokonać/naprawić pomimo realnych i dużych trudności przy dołożeniu realnego i dużego nakładu czasu i wysiłku. (4)- **poważne naruszenie**- osoba, której dane dotyczą, może napotkać poważne i nieodwracalne konsekwencje, mimo nakładu czasu i wysiłku.	
1		1	- bycie ofiarą szantażu	**M**
2		2	- dyskryminacja	**M**
1		2	- kradzież tożsamości	**M**
1		1	- możliwość utraty kontroli nad danymi	**M**
2		2	- naruszenie dobrego imienia	**M**
2		2	- naruszenie dóbr osobistych	**M**
2		2	- naruszenie poufności danych osobowych, chronionych tajemnicą zawodową	**M**
1		1	- poczucie naruszenia fundamentalnych praw człowieka	**M**
3		3	- poczucie wkroczenia w sferę prywatności	**Ś**
1		2	- problemy w relacjach prywatnych lub służbowych (wizerunek, utrata reputacji, utrata anonimowości)	**M**
1		1	- separacja lub rozwód	**M**
1		1	- utrata pieniędzy w wyniku oszustwa	**M**
1		1	- uprowadzenie	**M**
1		1	- utrata pacy	**M**
1		1	- utrata więzi rodzinnych	**M**
2		2	-zastraszenie (w mediach społecznościowych)	**M**
2		3	- zniesławienie	**M**
1		1	- pozbawienie praw osób, których dane dotyczą	**M**

PROCES OCENY DPIA		WYNIK OCENY DPIA			
Postępowanie z ryzykiem **Środki, których podjecie jest planowane w celu zaradzenia ryzykiem**		**Ocena ryzyka szczątkowego**	**Postępowanie z ryzykiem**		**Konieczność przeprowadzenia konsultacji**
	Czy podmiot medyczny stosuje kodeksy postępowania, o których mowa w art. 40 RODO ? TAK/NIE	Należy wskazać czy poziom ryzyka jest akceptowalny (po zastosowaniu środków minimalizujących ryzyko)	Należy wskazać, jaką decyzję podejmuje się w związku z oszacowaniem ryzykiem. Czy podejmuje się decyzje o: 1) **AKCEPTACJI**- ryzyko przedstawia wartość akceptowalną. 2) **MODYFIKACJI**- zaplanowane dodatkowe środki techniczne i organizacyjne w celu zmniejszenia prawdopodobieństwa wystąpienia negatywnego zdarzenia. 3)**UNIKANIU**- rezygnacja z danej czynności przetwarzania. 4) **DZIELENIU**- podjecie decyzji o wykupieniu dodatkowego ubezpieczenia w zakresie danej czynności (scedowanie skutków naruszenia).		W przypadku, gdy ryzyko naruszenia praw i wolności osób fizycznych, zostało oszacowane jako wysokie należy skonsultować się z organem nadzoru- art. 36 RODO
- aktualizacja regulacji wewnętrznych	**TAK**	**Małe**	Akceptuje się ryzyko.	Nie ma konieczności podejmowania dalszych działań.	**NIE**
- aktualizacja procesów identyfikacji pacjentów					
- kontrola dostępu do danych osobowych					
- anonimizacja		**Średnie**	Akceptuj się ryzyko lub je modyfikuje.	Podejmuje się działania mające na celu zredukowanie tego poziomu za pomocą modyfikacji.	**NIE**
- archiwizacja					
- automatyczne blokowanie urządzeń/konserwacja urządzeń					
- aktualizacja (aneksowanie) aktualnych umów z placówkami współpracującymi (SPZOZ, NZOZ, laboratoria)		**Wysokie**	Modyfikuje się ryzyko lub unika się ryzyka.	Podejmuje się działania mające na celu zredukowanie tego poziomu za pomocą: - modyfikacji, - unikania.	**TAK**
- kopie zapasowe					
- systematyczne zapisywanie danych na dodatkowych zabezpieczonych nośnikach					
- korzystanie z licencjonowanego oprogramowania		**Bardzo wysokie**	Modyfikuje się ryzyko i/lub dzieli się ryzyko lub unika się ryzyka.	Podejmuje się działania mające na celu zredukowanie	**TAK**
- ograniczenie dostępu do danych osobowych					
- okresowe przeglądu uprawnień w systemach					

- stosowanie nowych klauzul informacyjnych - oprogramowanie antywirusowe - szkolenia dla nowych pracowników - sprawdzanie zabezpieczeń fizycznych				tego poziomu za pomocą: - modyfikacji, - unikania, - dzielenia.	

DYREKTOR CENTRUM

Joanna Chromiec

ARKUSZ ZARZĄDZANIA RYZYKIEM						
NAZWA STANOWISKA:						
l.p.	**Ryzyko**	**Prawdopodobieństwo wystąpienia ryzyka (skala 1-4 pkt)**	**Skutek (skala 1-4 pkt)**	**Poziom wpływu ryzyka na bezpieczeństwo (Istotność ryzyka) (skala 1-16 pkt)**	**Ocena ryzyka – wynik (dopuszczalność)**	**Propozycje reakcji na ryzyko**
1.	Nieuprawniony dostęp do pomieszczenia			Ryzyko nieznaczne	Dopuszczalne (akceptowane)	Systematyczne monitorowanie ryzyka
2.	Ujawnienie haseł dostępu do stanowiska komputerowego			Ryzyko nieznaczne	Dopuszczalne (akceptowane)	Systematyczne monitorowanie ryzyka
3.	Nieuprawnione przeniesienie informacji na inny nośnik			Ryzyko nieznaczne	Dopuszczalne (akceptowane)	Systematyczne monitorowanie ryzyka
4.	Utrata nośnika zawierającego dane osobowe			Ryzyko nieznaczne	Dopuszczalne (akceptowane)	Systematyczne monitorowanie ryzyka
5.	Nieuprawnione wyniesienie danych osobowych zawartych na nośniku elektronicznym			Ryzyko nieznaczne	Dopuszczalne (akceptowane)	Systematyczne monitorowanie ryzyka
6.	Atak wirusa			Ryzyko nieznaczne	Dopuszczalne (akceptowane)	Systematyczne monitorowanie ryzyka
7.	Klęska żywiołowa, wypadek, zdarzenie, w wyniku których utracono poufność danych osobowych			Ryzyko nieznaczne	Dopuszczalne (akceptowane)	Systematyczne monitorowanie ryzyka
8.	Włamanie do systemu komputerowego w tym do stanowiska komputerowego lub urządzenia mobilnego			Ryzyko umiarkowane	Dopuszczalne (akceptowane)	Systematyczne monitorowanie ryzyka
9.	Błędy i pomyłki Użytkowników			Ryzyko nieznaczne	Dopuszczalne (akceptowane)	Systematyczne monitorowanie ryzyka
10.	Brak mechanizmów uniemożliwiających skasowanie lub zmianę logów przez administratora lub innego użytkownika			Ryzyko nieznaczne	Dopuszczalne (akceptowane)	Systematyczne monitorowanie ryzyka
11.	Awaria sprzętu			Ryzyko nieznaczne	Dopuszczalne (akceptowane)	Systematyczne monitorowanie ryzyka
12.	Brak w wykorzystywanych aplikacjach mechanizmów zapewniających integralność danych			Ryzyko nieznaczne	Dopuszczalne (akceptowane)	Systematyczne monitorowanie ryzyka

13.	Brak kontroli nad dokumentami w zakresie ich kopiowania i drukowania			Ryzyko nieznaczne	Dopuszczalne (akceptowane)	Systematyczne monitorowanie ryzyka
14.	Nieuprawnione wprowadzenie zmian w treści dokumentu			Ryzyko nieznaczne	Dopuszczalne (akceptowane)	Systematyczne monitorowanie ryzyka
15.	Błędy oprogramowania lub sprzętu			Ryzyko nieznaczne	Dopuszczalne (akceptowane)	Systematyczne monitorowanie ryzyka

.....

pieczęć i podpis inspektora ochrony danych osobowych

DYREKTOR CENTRUM

Joanna Chromiec

LEGENDA

Prawdopodobieństwo wystąpienia ryzyka	Ilość punktów	Przesłanki
(1)- **mało prawdopodobne.**	**1**	Raczej nie zdarzy się w ciągu roku, bądź prawdopodobieństwo jest mniejsze niż od 10%.
(2)- **możliwe.**	**2**	Raczej zdarzy się w ciągu roku, bądź prawdopodobieństwo zdarzenia wynosi powyżej 10% , ale poniżej 25%.
(3)- **prawdopodobne.**	**3**	Raczej zdarzy się w ciągu miesiąca, bądź prawdopodobieństwo zdarzenia wynosi powyżej 25% , ale poniżej 50%.
(4)- **wysokie prawdopodobieństwa lub pewność wystąpienia.**	**4**	Raczej zdarzy się w ciągu miesiąca, bądź prawdopodobieństwo zdarzenia wynosi powyżej 50%.

Skutek wystąpienia ryzyka	Ilość punktów	Przesłanki
Niski	1	Zakłócenie lub opóźnienie w wykonywaniu zadań. Bez uszczerbku dla wizerunku. Skutki łatwe do usunięcia
Średni	2	Spadek efektywności działania i obniżenie jakości wykonywania zadań. Niewielka strata finansowa. Nieznaczny negatywny wpływ na wizerunek. Trudny proces przywracania stanu poprzedniego
Wysoki	3	Duże zagrożenie realizacji kluczowych zadań albo osiągania założonych celów. Dotkliwa strata finansowa. Znaczny uszczerbek na wizerunku. Długotrwały i trudny proces przywracania stanu poprzedniego.
Bardzo wysoki	4	Poważna niezgodność z przepisami prawa. Brak procedur dla danego procesu. Olbrzymie zakłócenia pracy. Znaczny uszczerbek na wizerunku. Zagrożenia spowodują brak zachowania ciągłości procesów działania, utrzymania funkcjonalności systemów niezbędnych do wykonywania podstawowych celów. Brak osiągnięcia kluczowych celów. Straty finansowe.

Oszacowanie ryzyka	Dopuszczalność ryzyka	Działania
Ryzyko nieznaczne Skala: 1- 4 pkt	Dopuszczalne (akceptowane)	Zaleca się rozważenie możliwości dalszego zmniejszenia poziomu ryzyka lub zapewnienie, że ryzyko pozostanie na tym samym poziomie.
Ryzyko umiarkowane Skala: 5 - 8 pkt	Dopuszczalne (akceptowane)	Zaleca się zaplanowanie i podjęcie działań, których celem jest zdecydowane i skuteczne zmniejszenie ryzyka.
Ryzyko wysokie Skala: 9 – 12 pkt	Dopuszczalne (akceptowane)	Zaleca się zaplanowanie i podjęcie działań, których celem jest zdecydowane zmniejszenie ryzyka.
Ryzyko poważne Skala: 13 - 16 pkt	Niedopuszczalne (nieakceptowane)	Działania nie mogą być podjęte ani kontynuowane do czasu zmniejszenia ryzyka do poziomu dopuszczalnego.

DYREKTOR CENTRUM

Joanna Chromiec