Załącznik nr 1
do Zarządzenia nr 7
Dyrektora Ośrodka Leczenia Uzależnień
SP ZOZ w Lublinie
z dnia 17 czerwca 2015r.

Polityka bezpieczeństwa
w zakresie przetwarzania danych osobowych
w Ośrodku Leczenia Uzależnień SP ZOZ w Lublinie

Polityka Bezpieczeństwa przetwarzania danych osobowych w Ośrodku Leczenia Uzależnień SP ZOZ w Lublinie określa zbiór zasad bezpieczeństwa jako procedury regulujące sposób zarządzania danymi, ochroną i wymianą wewnątrz Ośrodka jak i na zewnątrz w kontaktach z instytucjami państwowymi, indywidualnymi pacjentami i pracownikami.
Dokument ten został opracowany na podstawie § 3 pkt. 1 i § 4 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnie 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych *(Dz. U. z 2004 r. Nr 100, poz. 1024)*, zwanego dalej Rozporządzeniem.

WPROWADZENIE I CEL POLITYKI BEZPIECZEŃSTWA

OLU SP ZOZ w Lublinie administruje danymi osobowymi w rozumieniu przepisów Ustawy o ochronie danych osobowych, a czynności w sprawach z zakresu ochrony danych osobowych określa i nadzoruje ich wykonywanie Dyrektor Ośrodka .
Administrator danych osobowych biorąc pod uwagę wagę problemów związanych z ochroną danych osób fizycznych powierzających Ośrodkowi swoje dane osobowe do właściwej i skutecznej ochrony deklaruje doskonalić i rozwijać nowoczesne metody przetwarzania danych. Deklaruje, że Ośrodek Leczenia Uzależnień będzie stale doskonalił i rozwijał organizacyjne, techniczne oraz informatyczne środki ochrony danych osobowych przetwarzanych zarówno metodami tradycyjnymi jak i elektronicznie.

Celem niniejszej Polityki Bezpieczeństwa jest wskazanie działań i określenie zasad przetwarzania danych osobowych oraz ich bezpieczeństwa poprzez ustalenie praw, reguł, procedur i praktycznych doświadczeń regulujących sposób ich zarządzania, ochrony i dystrybucji wewnątrz Ośrodka Leczenia Uzależnień SP ZOZ w Lublinie, jak i w kontaktach z otoczeniem.

Dokument ten odnosi się całościowo do problemu zabezpieczenia danych osobowych w Ośrodku Leczenia Uzależnień SP ZOZ w Lublinie.

Polityką bezpieczeństwa objęte są dane osobowe, którymi zgodnie z ustawą o ochronie danych osobowych (Dz.U. 2014 poz. 1182 - tekst jednolity) są wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;

Reguły i zasady do przetwarzania danych osobowych prowadzonych zarówno w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych obowiązują, także w przypadku przetwarzania danych poza zbiorem danych.

Zgodnie z Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r., Polityka Bezpieczeństwa zawiera w szczególności:

a) Wykaz budynków i pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
b) Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
c) Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania pomiędzy nimi,
d) Sposób przepływu danych pomiędzy poszczególnymi systemami,
e) Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

ZARZĄDZANIE PRZETWARZANIEM DANYCH OSOBOWYCH

1. Wykaz budynków i pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe

Komórki organizacyjne Ośrodka Leczenia Uzależnień SP ZOZ w Lublinie zlokalizowane są w Lublinie w budynkach przy ul. Karłowicza 1 i Al. Tysiąclecia 5.
Wykaz budynków i pomieszczeń, w których przetwarzane są dane osobowe oraz rodzaj i zakres przetwarzania danych przedstawia poniższa tabela

Tabela nr 1

Wykaz budynków i pomieszczeń OLU SP ZOZ w Lublinie, tworzących obszar, w którym przetwarzane są dane osobowe

Lp.	Budynek	Pomieszczenie	Komórka organizacyjna	Rodzaj przetwarzanych danych	Sposób przetwarzania
1.	Karłowicza 1 w Lublinie	Rejestracja	Administracja	Dane osobowe pacjentów	1,2,3,4,5,6
		Pokój nr 2	PLUDiM/PLU	Dane osobowe pacjentów	1,2,4,5
		Pokój nr 6	PLU	Dane osobowe pacjentów	1,2,4,5
		Pokój nr 7	PLU	Dane osobowe pacjentów	1,2,4,5,
		Pokój nr 8	PLU	Dane osobowe pacjentów	1,2,4,5
		Pokój nr 10	Z-ca dyrektora	Dane osobowe pacjentów	1,2,4,5
		Pokój nr 11	Dyrektor	Dane osobowe pacjentów i pracowników	1,2,4,5
		Pokój nr 12	Główny Księgowy	Dane osobowe pracowników	1,2,3,4,5,6,
		Pokój nr 102	PTUAiW	Dane osobowe pacjentów	1,2,3,4,5,6,
		Pokój nr 106	Administracja	Dane osobowe pracowników	1,2,3,4,5,6,
				Dane pacjentów	2,6
		Pokój nr 107	Administracja	Dane osobowe pracowników	1,2,3,4,5,6,
		Pokój nr 108	PTUAiW	Dane osobowe pacjentów	1,4,5,
		Pokój nr 110	PTUAiW	Dane osobowe pacjentów	1,4,5,
		Pokój nr 111	PTUAiW	Dane osobowe pacjentów	1,4,5,
		Pokój nr 112	PTUAiW	Dane osobowe pacjentów	1,4,5,
		Pokój nr 113	PTUAiW/ DOTUA	Dane osobowe pacjentów	1,4,5,
		Pokój nr 114	DOTUA	Dane osobowe pacjentów	1,4,5,
		Pokój nr 115	DOTUA	Dane osobowe pacjentów	1,4,5,
2.	Tysiąclecia 5	Rejestracja	Program Terapii Substytucyjnej	Dane osobowe pacjentów	1,3,
		Pokój Terapeutów	Program Terapii Substytucyjnej	Dane osobowe pacjentów	1,2,3,4,5
		Pokój lekarski	Program Terapii Substytucyjnej	Dane osobowe pacjentów	2,4,6

LEGENDA: 1. zbieranie, 2. utrwalanie, 3. przechowywanie, 4. opracowywanie, 5. zmienianie, 6. udostępnianie, 7. usuwanie

2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

Wykaz zbiorów danych osobowych opracowano w oparciu o Jednolity Rzeczowy Wykaz Akt OLU SP ZOZ w Lublinie, stanowiący Załącznik do Instrukcji Kancelaryjnej dla Ośrodka .
Nazwy zbiorom nadano zgodnie z hasłem klasyfikacyjnym pierwszej, drugiej i trzeciej klasy.
Ośrodek Leczenia Uzależnień SP ZOZ w Lublinie realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych sprawuje nadzór nad rodzajami oraz zawartością zbiorów danych osobowych tworzonych na jego obszarze.

Wykaz zbiorów danych osobowych wraz ze wskazaniem sposobu gromadzenia danych i nazwy programu, w którym są przetwarzane:

Tabela nr 2

Lp.	Nazwa zbioru danych osobowych (hasło klasyfikacyjne)	Sposób gromadzenia	Nazwa programu
1.	**ORGANIZACJA I ZARZĄDZANIE** Akty normatywne. Prognozowanie, Planowanie, Sprawozdawczość i Statystyka. Informatyka. Współdziałanie, Kontakty Nadzór, Kontrole	Forma papierowa. Forma elektroniczna.	System Informatyczny: Kadowo-Płacowy -GRATYFIKANT Księgowo-Rachunkowy -REWIZOR Ubezpieczeniowy - PŁATNIK - System operacyjny Windows (MS Office – Excel, Word)
2.	**DZIAŁALNOŚĆ MERYTORYCZNA** Działalność merytoryczna - dokumentacja indywidualna pacjentów - PLU - PTUAiW - DOTUA - Programu Terapii Substytucynej - dokumentacja zbiorcza - księga główna - wydruki z rejestru komputerowego Dokumentacja dotycząca udzielanych w OLU SP ZOZ w Lublinie świadczeń zdrowotnych Dokumentacja związana z działalnością Programu Terapii Substytucyjnej	Forma elektroniczna. Forma papierowa.	System KS-PPS – rozliczenia System SZOI (Windows – MS Office – Excel, Word)
3.	**KADRY.** Akta osobowe Ewidencja akt osobowych Zatrudnienie i wynagradzanie.	Forma papierowa. Forma elektroniczna.	GRATYFIKANT - system kadrowo-płacowy,

	Szkolenie pracowników. Dyscyplina pracy, urlopy, kary. Sprawy socjalno – bytowe. Ubezpieczenia osobowe. - Pomoc socjalno-bytowa - Dofinansowania i zapomogi - opieka zdrowotna - Ubezpieczenia społeczne - składki ubezpieczenia spolecznego Bezpieczeństwo i higiena pracy. - szkolenia Wypadki przy pracy, choroby Zawodowe - profilaktyka zapobiegawcza - badania okresowe		Windows – MS Office – Excel, Word)
4.	**BUDŻET, PODATKI, RACHNKOWOŚĆ** Podatki i opłaty Rachunkowość, księgowość, obsługa kasowa · księgowość · płace - rozliczenia, diety, ubezpieczenia - dokumentacja wynagrodzeń za umowy zlecenia i o dzieło - deklaracje podatkowe PIT - ustalanie i odprowadzanie składek ubezpieczenia społecznego - naliczanie kapitału początkowego Zamówienia publiczne	Forma papierowa. Forma elektroniczna.	REWIZOR - system finansowo-księgowy, PŁATNIK – program ubezpieczeniowy, GRATYFIKANT- s. kadrowo-placowy, Windows – MS Office – Excel, Word)

Ośrodek Leczenia Uzależnień SP ZOZ w Lublinie realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych zapewnia zgodną z przepisami rozdziału 5 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych ochronę zbiorom danych osobowych sporządzanym doraźnie, wyłącznie ze względów technicznych, szkoleniowych lub w związku z dydaktyką prowadzenia zajęć z pacjentami realizowanymi w Ośrodku , a po ich wykorzystaniu niezwłocznie usuwanych albo poddanych anonimizacji.

Ośrodek Leczenia Uzależnień SP ZOZ w Lublinie realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych zabrania tworzenia zbiorów danych osobowych, a także gromadzenia w zbiorach lub poza nimi kategorii danych osobowych innych niż niezbędne dla realizacji celów statutowych Ośrodka.

3. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania pomiędzy nimi.

Dane osobowe w Ośrodku Leczenia Uzależnień gromadzone są w systemach informatycznych, na zewnętrznych nośnikach danych oraz w zbiorach dokumentów papierowych.
Rozwiązania techniczne w systemach informatycznych pozwalają na uzupełnianie tych samych danych z innych posiadanych zasobów w ramach jednostki, co przekłada sie na ich efektywniejsze wykorzystanie w załatwianiu spraw. Zakres gromadzonych danych osobowych jest zgodny z przepisami prawa.

Tabela nr 3

Struktura zbioru zawierającego informacje o pracownikach, zatrudnieniu i wynagrodzeniu.

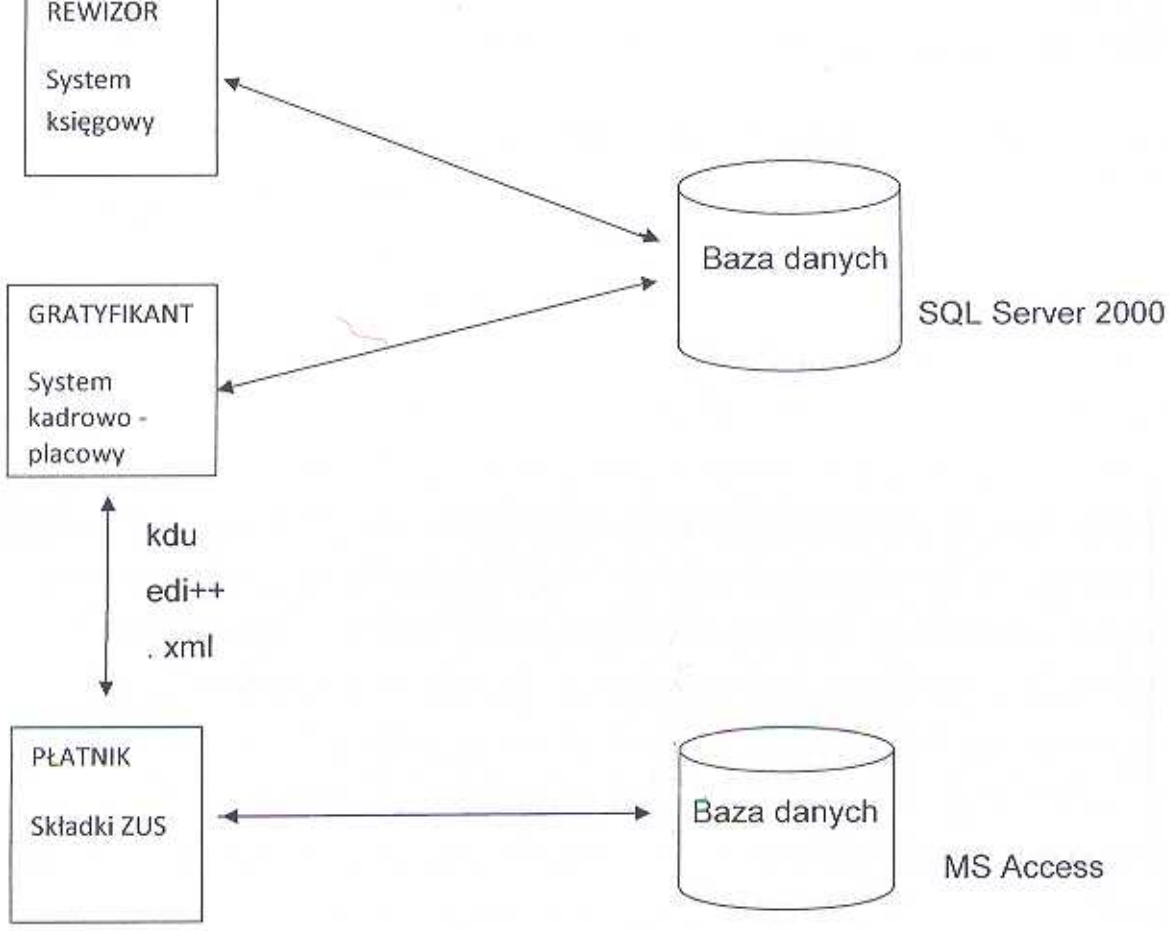
KADRY	Ewidencja	Dane osobowe	Imię i nazwisko, PESEL, data i miejsce urodzenia, imię ojca i matki, stan cywilny, płeć, adres zamieszkania, itp.
		Pozostałe dane	Dokument tożsamości, dane ubezpieczeniowe, rozliczeniowe – nr konta w banku, badania okresowe, kursy bhp itp.
	Zatrudnienie	Umowa o pracę	Pracownik – imię i nazwisko, adres zamieszkania, umowa nr na czas, aneksy
		Umowa cywilnoprawna	Pracownik – imię nazwisko, data umowy, nr dowodu tożsamości, adres zamieszkania, umowa- tytuł, rachunek na kwotę
PŁACE	Wypłaty	Umowy o pracę	Listy płac
		Umowy cywilnoprawne	Rachunki za świadczone usługi
INNE:	ZFŚS	Zapomogi , dofinansowanie – pracownik – imię i nazwisko, świadczenie	

Struktura zbioru zawierającego informacje o pacjentach, historia choroby i przeprowadzona terapia.

dane pacjenta:	[**pacjent** - imię, nazwisko, adres (kod pocztowy, miejscowość, ulica, nr domu/mieszkania), dane identyfikacyjne(Pesel,]
Udzielenie świadczenia zdrowotnego pacjentowi:	[pacjent - imię i nazwisko, data udzielanego świadczenia, rozpoznanie główne, rozpoznanie współistniejące i okres leczenia] Lekarz, terapeuta – imię i nazwisko , pesel, numer prawa wykonywania zawodu, data udzielonego świadczenia, rodzaj udzielonego świadczenia
Przeprowadzona terapia i zastosowane leki:	[historia choroby pacjenta]

4. Sposób przepływu danych pomiędzy poszczególnymi systemami

Gromadzenie danych następuje przez pozyskiwanie ich z danych źródłowych, a także z innych zasobów. Gromadzone dane osobowe są udostępniane pracownikom w zakresie niezbędnym do ich pracy i wynikającym z przepisów prawa poprzez posiadane systemy informatyczne. Dane udostępniane są poprzez moduły do przeglądania danych, np. przeglądarki, zewnętrzny plik wymiany baz danych. Możliwość wglądu przez pracowników w dane osobowe pozwala na ich porównywanie i sprostowanie ewentualnych rozbieżności ograniczając jednocześnie ilość wyjaśnień. Udostępnianie danych upoważnionym pracownikom w OLU SP ZOZ w Lublinie możliwe jest za pośrednictwem serwera na którym zainstalowane są systemy: finansowo-księgowy – REWIZOR, kadrowo – płacowy GRATYFIKANT i program PŁTNIK.
Do serwera podłączone są trzy komputery w administracji i głównej księgowej.
Rewizor i Gratyfikant korzystają z bazy danych w systemie SQL Serwer 2000,
Program PŁATNIK korzysta z bazy danych w systemie MS Access.
Dane do tych systemów wprowadzone zostały ręcznie lub za pomocą przenośnego dysku przez obsługujących, upoważnionych pracowników OLU.
Współpraca między Gratyfikantem a Płatnikiem może przebiegać za pomocą plików o rozszerzeniu kdu, za pomocą edi++ - systemu wymiany dokumentów i dokumentów .xml. Obecnie nie korzysta się z tej możliwości.
Pozostałe systemy i programy używane do przetwarzania danych osobowych w OLU SP ZOZ w Lublinie bazują na danych wprowadzonych przez pracowników i są to systemy zamknięte (dotyczą najczęściej komputerów znajdujących się w gabinetach terapeutów).
Systemy NFZ, tj. KS-PPS i SZOI, do których mają dostęp upoważnieni pracownicy Ośrodka współpracują ze sobą w przepływie danych osobowych w sieci informatycznej Narodowego Funduszu Zdrowia.



Rys. Przepływ danych w sieci lokalnej OLU SP ZOZ w Lublinie

5. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności i integralności i rozliczalności przy przetwarzaniu danych

OLU SP ZOZ w Lublinie przetwarza dane osobowe na podstawie przepisów prawa. Dane osobowe mogą być udostępnianie zgodnie z art.29 ustawy z dnia 29 sierpnia 1997r o ochronie danych osobowych (Dz.U. 2014 poz. 1182 - tekst jednolity).
Charakter oraz ilość przetwarzanych danych w OLU, powoduje konieczność ich ochrony przed nieautoryzowanym dostępem, utratą poufności, nieuprawnioną modyfikacją. Podejmowane są działania służące zachowaniu ich integralności i rozliczalności. W celu zapewnienia ochrony danych osobowych stosuje sie odpowiednie rozwiązania organizacyjne i techniczne.

1. Budynek OLU objęty jest systemem kontroli dostępu, w tym sygnalizacji włamania.
2. Elektroniczne systemy monitoringu pozwalają na kontrole ruchu osób i informują Firmę Ochrony o przypadkach nieautoryzowanego wejścia.
3. Każdy pracownik OLU przed dopuszczeniem do przetwarzania danych osobowych zobowiązany jest do zapoznania się oraz stosowania przepisów ustawy o ochronie danych osobowych.

A. Środki Organizacyjne

a. Osoby przetwarzające dane osobowe

W Ośrodku Leczenia Uzależnień SP ZOZ w Lublinie w procesie zarządzania i przetwarzania danych osobowych biorą udział następujące osoby:

1) Administrator danych osobowych w OLU SP ZOZ w Lublinie, którym jest Dyrektor Ośrodka;
2) Pełnomocnik ds. bezpieczeństwa informacji – osoba wyznaczona przez administratora danych realizująca zadania w zakresie przestrzegania bezpieczeństwa danych osobowych przetwarzanych w Ośrodku w sposób tradycyjny i w systemach informatycznych
3) Administrator systemów informatycznych – osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych, jak też za sprawne działania baz danych zawierających dane osobowe,
4) Osoby upoważnione (użytkownicy) osoby posiadające upoważnienie wydane przez administratora danych lub osobę przez niego wyznaczoną i dopuszczone w zakresie wskazanym w tym upoważnieniu do przetwarzania danych osobowych w sposób tradycyjny i w systemie informatycznym danej komórki organizacyjnej.

b. Procedury nadawania uprawnień do przetwarzania danych osobowych.

Do przetwarzania danych, zgodnie z art. 37 ustawy mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych. W imieniu Dyrektora OLU SP ZOZ w Lublinie, Pełnomocnik ds. bezpieczeństwa informacji prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, która zawiera:

1) Imię i nazwisko osoby upoważnionej;
2) Datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych;
3) Zakres nadanego upoważnienia
4) Identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

Upoważnienia do przetwarzania danych osobowych wydawane są na podstawie „Zakresu obowiązków, praw i odpowiedzialności" pracownika zatrudnianego w OLU SP ZOZ w Lublinie , w którym zawierają się czynności, które wymagają przetwarzania danych osobowych pracownika bądź pacjenta.
Dopuszcza się możliwość upoważniania do przetwarzania danych osobowych osób będących pracownikami firm zewnętrznych, które wykonują zadania na rzecz OLU w Lublinie, w obszarze gdzie przetwarza się dane osobowe, wynikające z zawartej umowy. Pełnomocnik ds. bezpieczeństwa informacji kieruje wniosek o wydanie upoważnienia do Administratora danych osobowych.

c. Zasady przestrzegane przy przetwarzaniu danych osobowych

W pomieszczeniach Ośrodka, w których przetwarzane są dane osobowe należy przestrzegać następujących zasad:

1) W pomieszczeniach Ośrodka, w którym przetwarzane są dane osobowe mają prawo przebywać wyłącznie osoby upoważnione do dostępu i/lub przetwarzania danych osobowych oraz osoby sprawujące nadzór i kontrolę nad bezpieczeństwem przetwarzania tych danych (wzór upoważnienia stanowi załącznik nr 2 do „Instrukcji zarządzania systemem informatycznym...).
2) Osoby nie upoważnione do przetwarzania danych osobowych określonej kategorii, mające interes prawny lub faktyczny w uzyskaniu dostępu do tych danych lub wykonujące inne czynności nie mające związku z dostępem do tych danych mogą przebywać w pomieszczeniach OLU SP ZOZ, w którym przetwarzane są dane osobowe - wyłącznie w obecności upoważnionego pracownika Ośrodka, lub – w razie jego nieobecności - na podstawie upoważnienia wydanego przez administratora danych osobowych lub inną upoważnioną osobę.
3) Całkowite opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe, musi wiązać się z zastosowaniem dostępnych środków zabezpieczających to pomieszczenie przed wejściem osób niepowołanych.
4) Chwilowe opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe, musi wiązać się z zastosowaniem dostępnych środków zabezpieczających używane aktualnie zbiory danych osobowych. W szczególności w razie planowanej, choćby chwilowej, nieobecności pracownika upoważnionego do przetwarzana danych osobowych obowiązany jest on umieścić zbiory występujące w formach tradycyjnych w odpowiednio zabezpieczonym miejscu ich przechowywania oraz dokonać niezbędnych operacji w systemie informatycznym uniemożliwiającym dostęp do danych osobowych osobom niepowołanym.
5) Opuszczenie przez pracownika przetwarzającego dane osobowe obszaru ich przetwarzania bez zabezpieczenia pomieszczenia oraz umiejscowionych w nim zbiorów danych jest niedopuszczalne, i jako takie traktowane będzie, jako ciężkie naruszenie podstawowych obowiązków pracowniczych.

d. Zasady postępowania w przypadku naruszenia ochrony danych osobowych

Każdy pracownik biorący udział w przetwarzaniu danych osobowych w systemie informatycznym jest odpowiedzialny za bezpieczeństwo tych danych. W szczególności osoba, która zauważyła zdarzenie mogące być przyczyną naruszenia ochrony danych osobowych lub mogące spowodować naruszenie bezpieczeństwa danych, zobowiązana jest do natychmiastowego poinformowania pełnomocnika ds. bezpieczeństwa informacji lub administratora systemu informatycznego.

O naruszeniu ochrony danych osobowych mogą świadczyć następujące symptomy:

1. brak możliwości uruchomienia przez użytkownika aplikacji pozwalającej na dostęp do danych osobowych,
2. brak możliwości zalogowania się do tej aplikacji,
3. ograniczone, w stosunku do normalnej sytuacji, uprawnienia użytkownika w aplikacji (na przykład brak możliwości wykonania pewnych operacji normalnie dostępnych użytkownikowi) lub uprawnienia poszerzone w stosunku do normalnej sytuacji,
4. wygląd aplikacji inny niż normalnie,
5. inny zakres danych niż normalnie dostępny dla użytkownika – dużo więcej lub dużo mniej danych,
6. znaczne spowolnienie działania systemu informatycznego,

7. pojawienie się niestandardowych komunikatów generowanych przez system informatyczny,
8. ślady włamania lub prób włamania do obszaru, w którym przetwarzane są dane osobowe,
9. ślady włamania lub prób włamania do pomieszczeń, w których odbywa się przetwarzanie danych osobowych, w szczególności do pokoju , w którym jest serwer,
10. włamanie lub próby włamania do szafek, w których przechowywane są – w postaci elektronicznej lub papierowej – nośniki danych osobowych,
11. zagubienie bądź kradzież nośnika danych osobowych,
12. zagubienie bądź kradzież nośnika materiału kryptograficznego (karty mikroprocesorowej, dyskietki itp.),
13. kradzież sprzętu informatycznego, w którym przechowywane są dane osobowe,
14. informacja z systemu antywirusowego o zainfekowaniu systemu informatycznego wirusami,
15. fizyczne zniszczenie lub podejrzenie zniszczenia elementów systemu informatycznego przetwarzającego dane osobowe na skutek przypadkowych lub celowych działań albo zaistnienia działania siły wyższej,

W wypadku wystąpienia powyższych symptomów, jak również innych objawów, które zdaniem pracownika mogą wskazywać na zagrożenie bezpieczeństwa danych osobowych, należy natychmiast powiadomić pełnomocnika ds. bezpieczeństwa informacji lub administratora systemu informatycznego.

Po otrzymaniu zgłoszenia o wystąpieniu symptomów wskazujących na możliwość zaistnienia w OLU naruszenia bezpieczeństwa danych osobowych Pełnomocnik ds. bezpieczeństwa informacji , we współpracy z Administratorem systemu informatycznego, jest zobowiązany do podjęcia kroków w celu:

a) wyjaśnienia zdarzenia, a w szczególności czy miało miejsce naruszenie ochrony danych osobowych,
b) wyjaśnienia przyczyn naruszenia bezpieczeństwa danych osobowych i zebranie ewentualnych dowodów, a w szczególności, gdy zdarzenie było związane z celowym działaniem pracownika bądź osób trzecich,
c) zabezpieczenia systemu informatycznego przed dalszym rozprzestrzenianiem się zagrożenia,
d) usunięcia skutków incydentu i przywróceniu pierwotnego stanu systemu informatycznego (to jest stanu sprzed incydentu).

Pełnomocnik ds. bezpieczeństwa informacji we współpracy z administratorem systemu informatycznego podejmuje działania zmierzające do wyjaśnienia zgłoszonego zdarzenia:

- przeprowadzenia analizy poprawności funkcjonowania systemu informatycznego,
- przeprowadzenie analizy danych osobowych przetwarzanych w systemie informatycznym,
- zabezpieczenie danych przetwarzanych w systemie informatycznym, w szczególności danych konfiguracyjnych tego systemu.

Pełnomocnik ds. bezpieczeństwa informacji określa na podstawie zebranych informacji przyczyny zaistnienia incydentu. Jeżeli incydent był spowodowany celowym działaniem, jest on zobowiązany do pisemnego powiadomienia administratora danych osobowych w OLU, który może poinformować organy uprawnione do ścigania przestępstw o fakcie celowego naruszenia bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym.

System informatyczny, którego prawidłowe działanie zostało odtworzone powinien zostać poddany szczegółowej obserwacji w celu stwierdzenia całkowitego usunięcia symptomów incydentu.
Pełnomocnik ds. bezpieczeństwa informacji prowadzi ewidencję interwencji związanej z zaistniałymi incydentami w zakresie bezpieczeństwa danych osobowych.
Ewidencja taka obejmuje następujące informacje:

- imię i nazwisko osoby zgłaszającej incydent,
- imię i nazwisko osoby przyjmującej zgłoszenie incydentu,
- datę zgłoszenia incydentu,
- przeprowadzone działania wyjaśniające przyczyny zaistnienia incydentu,
- wyniki przeprowadzonych działań,
- podjęte akcje naprawcze i ich skuteczność.

Pełnomocnik ds. bezpieczeństwa informacji odpowiedzialny jest za przeprowadzenie przynajmniej raz w roku analizy zaistniałych incydentów w celu:

- określenia skuteczności podejmowanych działań wyjaśniających i naprawczych,
- określenie wymaganych działań zwiększających bezpieczeństwo systemu informatycznego i minimalizujących ryzyko zaistnienia incydentów,
- określenie potrzeb w zakresie szkoleń administratorów systemu i użytkowników systemu informatycznego przetwarzającego dane osobowe.

B. Środki Techniczne

a. Kontrola dostępu – Ochrona fizyczna pomieszczeń

Dostęp do pomieszczeń Ośrodka Leczenia Uzależnień SP ZOZ w Lublinie, w których przetwarzane są dane osobowe podlega kontroli, tj.:

1) Kontrola dostępu polegać może w szczególności na ewidencjonowaniu wszystkich przypadków pobierania i zwrotu kluczy do pomieszczeń. W ewidencji uwzględnia się: imię i nazwisko osoby pobierającej lub zdającej klucz, numer lub inne oznaczenie pomieszczenia oraz godzinę pobrania lub zdania klucza.
2) Klucze do pomieszczeń, w których przetwarzane są dane osobowe wydawane być mogą wyłącznie pracownikom upoważnionym do przetwarzania danych osobowych lub innym pracownikom upoważnionym do dostępu do tych pomieszczeń na innych zasadach.
3) Ośrodek Leczenia Uzależnień realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych może wprowadzać inne formy monitorowania dostępu do obszarów przetwarzania danych osobowych.
4) Szczegółowe zasady kontroli dostępu do poszczególnych pomieszczeń Ośrodka Leczenia Uzależnień, w których przetwarzane są dane osobowe określane są przez osoby kierujące poszczególnymi jednostkami organizacyjnymi Ośrodka, w których takie obszary występują.

b. Postępowanie w zakresie komunikacji w sieci komputerowej.

1) Podłączenie sprzętu komputerowego do sieci teleinformatycznej wykonuje Administrator systemu informatycznego na polecenie Dyrektora OLU.
2) Zasoby informatyczne mogą być wykorzystywane tylko do wykonywania obowiązków służbowych.

3) Komunikacja pomiędzy pracownikami następuje poprzez katalogi udostępnione w sieci, na serwerze.

Środki techniczne i organizacyjne zostały określone w „Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Ośrodku Leczenia Uzależnień SP ZOZ w Lublinie" wprowadzonej zarządzeniem Dyrektora.

c. Ochrona danych osobowych przetwarzanych w formie elektronicznej.

Uwzględniając kategorie przetwarzanych danych wprowadza się w OLU wysoki poziom bezpieczeństwa ochrony danych osobowych. Poziom wysoki stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego, połączone jest z siecią publiczną.

1) System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem. W przypadku zastosowania logicznych zabezpieczeń, obejmują one kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną, oraz kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych;
2) Stosuje się mechanizmy kontroli dostępu do danych osobowych, wprowadzając w tym systemie, rejestrowany dla każdego użytkownika odrębny identyfikator. Dostęp do danych jest możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia przez wprowadzenie hasła;
3) System informatyczny służący do przetwarzania danych osobowych zabezpiecza się przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
4) Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przed utratą spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem. Usuwa się niezwłocznie po ustaniu ich użyteczności;
5) Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do likwidacji należy wcześniej pozbawić zapisów tych danych. W przypadku, gdy nie jest to możliwe, uszkodzić w sposób uniemożliwiający ich odczytanie;
6) W razie konieczności naprawy zachować szczególną ostrożność, aby nie doszło do ujawnienia danych osobowych. Ostatecznie pozbawić wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie zgodnie z zaleceniami Instrukcji Zarządzania Systemami Informatycznymi służącymi do przetwarzania danych osobowych w OLU SP ZOZ w Lublinie;
7) Pracownik OLU użytkujący komputer przenośny zawierający dane osobowe powinien zachować szczególną ostrożność podczas jego transportu i przechowywania poza obszarem przetwarzania danych osobowych po odpowiednio uzyskanej zgodzie.

UWAGA: *Szczegółowe zasady, procedury postępowania i środki bezpieczeństwa podczas przetwarzania i gromadzenia danych osobowych w formie elektronicznej zawarte są w „Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w OLU SP ZOZ w Lublinie"*

d. Środki ochrony w zakresie zabezpieczenia sprzętowego.

1) Do przetwarzania danych osobowych zastosowany został wysokiej klasy sprzęt informatyczny;
2) Serwer wyposażony w pamięć operacyjną z detekcją błędów;
3) Równoległy zapis na dyskach;
4) Zasilanie awaryjne serwerów i stacji roboczych UPS;
5) Sieć lokalna;

e. Środki ochrony w ramach oprogramowania systemu.

1) Zbiory danych osobowych oraz programy służące do przetwarzania danych osobowych są zabezpieczane przed przypadkową utratą albo celowym zniszczeniem poprzez wykonywanie kopii zapasowych;
2) W celu ochrony zbiorów danych osobowych prowadzonych w systemach informatycznych przed nieuprawnionym dostępem stosuje się mechanizmy kontroli dostępu do tych danych;
3) System informatyczny pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu;
4) W celu zapewnienia rozliczalności operacji dokonywanych przez użytkowników systemu informatycznego, w systemie tym dla każdego użytkownika rejestrowany jest odrębny identyfikator i hasło;
5) Ograniczone logowanie do systemu na koncie użytkownika uprzywilejowanego;
6) Rejestracja nieudanych prób logowania do systemu;
7) Logowanie wszystkich wykonywanych czynności;
8) W celu ochrony systemu przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego stosuje się oprogramowanie antywirusowe z automatyczną aktualizacją;
9) Oprogramowanie antywirusowe jest stale aktywne, baza definicji wirusów regularnie aktualizowana;
10) Kontrola antywirusowa powinna być przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie jak i do celów instalacyjnych.

f. Ochrona danych osobowych przetwarzanych w formie papierowej.

Dane osobowe przetwarzane i gromadzone przy użyciu tradycyjnych środków pisarskich gromadzone są w rejestrach, księgach, zeszytach papierowych oraz segregatorach. Dane te należy przechowywać w szafach zamykanych na zamek patentowy oraz w sejfach i kasetkach.

Obszar przetwarzania i gromadzenia danych osobowych zabezpiecza się przed dostępem osób nieuprawnionych. Przebywanie osób nieupoważnionych w obszarze przetwarzania danych jest dopuszczalne za zgodą administratora danych w obecności osób upoważnionych do przetwarzania danych osobowych.

Sposób postępowania z kluczami do pomieszczeń i szaf został opisany w punkcie poświęconym ochronie fizycznej pomieszczeń, w których przetwarza się dane osobowe.

6. Udostępnianie danych osobowych.

Udostępnianie danych osobowych w działaniach służbowych dopuszczalne jest tylko pracownikom posiadającym odpowiednie upoważnienie i zakres upoważnienia dostępu do danych osobowych pracownika lub pacjenta.
Udostępnienie danych osobowych zainteresowanego pracownika może nastąpić tylko w obecności pracownika administracji upoważnionego do dostępu do tego zakresu danych osobowych.
Udostępnienie danych pacjenta określa „Instrukcja postępowania w sprawie udostępniania dokumentacji medycznej"

ODPOWIEDZIALNOŚĆ KARNA I DYSCYPLINARNA.

1) Osoby mające dostęp do danych osobowych są zobligowane do stosowania niezbędnych środków zapobiegających ujawnieniu tych danych osobom nieupoważnionym. Zachowanie tajemnicy obowiązuje zarówno podczas trwania stosunku pracy jak i po jego ustaniu.
2) Naruszenie przepisów o ochronie danych osobowych jest zagrożone sankcjami karnymi określonymi w art. 49 - 54 ustawy oraz w art. 130, 266 – 269, 287 Kodeksu karnego;
3) Niezależnie od odpowiedzialności przewidzianej w przepisach, o których mowa w ust. 1, naruszenie zasad ochrony danych osobowych obowiązujących w Ośrodku Leczenia Uzależnień SP ZOZ w Lublinie może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

DYREKTOR
Ośrodka Leczenia Uzależnień
SP ZOZ w Lublinie
mgr Paweł Bijak

Inspektor
ds Pracowniczych
mgr Mirosław Rachycki

Kancelaria Radcy Prawnego
Beata Kowalska
20-023 Lublin, ul. Chopina 26/7
NIP 712 145 47 55