Szkolenie z zakresu Ochrony Danych Osobowych dla Studentów odbywających praktyki w Samodzielnym Publicznym Zespole Opieki Zdrowotnej w Sanoku

SPIS TREŚCI

1. RODO

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2016/679 z 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 95/45/WE (ogólne rozporządzenie o ochronie danych osobowych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1).

RODO został wprowadzone w celu zrównoważenie stopnia ochrony danych osobowych obywateli w państwach członkowskich UE.

RODO stosowane jest od dnia 25 maja 2018 r. we wszystkich państwach członkowskich UE.

Przepisy krajowe regulujące ochronę danych osobowych:

a) Ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych Dz.U.2018.1000 z dnia 24.05.2018;
b) Ustawy sektorowe np.:
- Ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta,
- Ustawy o działalności leczniczej,
- Ustawa o zawodach lekarza i lekarza dentysty,
- Ustawa o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych

Regulacje wewnętrzne SP ZOZ:

„Polityka ochrony danych osobowych w Samodzielnym Publicznym Zespole Opieki Zdrowotnej w Sanoku" wprowadzona do stosowania Zarządzeniem Dyrektora nr SPZOZ/ZARZ/DA/56/2018.
Polityka zawiera procedury, których przestrzeganie jest niezbędne do zapewnienia bezpiecznego przetwarzania danych osobowych. Treść polityki jest dokumentem do użytku wewnętrznego i ujawniana jest tylko tym osobom, którym jest to niezbędne dla realizacji ich obowiązków w związku z przetwarzaniem danych osobowych.

2. DANE OSOBOWE

Artykuł 4 RODO definiuje dane osobowe jako informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, tj. osobie, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny (np. PESEL), dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

A więc, są to wszelkie informacje, które pozwolą ustalić tożsamość danej osoby fizycznej.

Danymi osobowymi nie będą pojedyncze informacje o dużym stopniu ogólności, np. nazwa ulicy i numer domu, wysokość wynagrodzenia chyba że zostaną połączone z inną informacją która pozwoli na zidentyfikowanie osoby np., wynagrodzenie + Jan Kowalski mieszkający na ul. Stawki 5 w Sanoku, wtedy wynagrodzenie stanie się informacja o tej osobie dane, które umożliwią przy niewielkim

nakładzie pracy zidentyfikowanie osoby (np. „Dyrektor SP ZOZ w Sanoku") osoba czarnoskóra + informacja, że mieszka we wsi Pocałunek (jedna taka wieś w Polsce i zamieszkuje ją 200 osób)

Dane osobowe dotyczą wyłącznie żywych osób fizycznych.

3. KATEGORIE DANYCH OSOBOWYCH

Wyróżnia się następujące rodzaje/kategorie danych osobowych:
a) **szczególne kategorie danych osobowych** (zwane również danymi wrażliwymi/sensytywnymi)

Do szczególnych kategorii danych osobowych zaliczamy:
- dane ujawniające pochodzenie rasowe lub etniczne,
- poglądy polityczne,
- przekonania religijne lub światopoglądowe,
- przynależność do związków zawodowych,
- **dane genetyczne**,
- dane biometryczne,
- **dane dotyczące zdrowia**,
- seksualności lub orientacji seksualnej.

Katalog danych szczególnych jest zamknięty, co oznacza, że nie można włączać do niego innych kategorii danych.

b) **tzw. dane osobowe zwykłe,** np.:
- imię i nazwisko,
- PESEL,
- adres zamieszkania,
- data urodzenia, płeć,
- imiona rodziców,
- wykształcenie,
- adres e-mail, nr telefonu,
- nr i seria dowodu osobistego,
- login internetowy.

Dane osobowe zwykłe stanowią otwarty katalog danych. To wszystkie pozostałe dane, których nie można zaliczyć do szczególnej kategorii danych (danych wrażliwych/sensytywnych).

c) **dane dotyczące wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa**.
przetwarzanie takich danych musi znajdować oparcie w przepisach prawa krajowego lub unijnego, co oznacza, że nawet za zgodą osoby nie możemy wymagać zaświadczenia o niekaralności, jeżeli wymóg ten nie wynika wprost z przepisów rangi ustawowej zobowiązujących osobę ubiegającą się o zatrudnienie do wykazania swojej niekaralności i dostarczenia w związku z tym stosownego dokumentu.

Niekaralność jest przewidywana w wielu ustawach jako warunek zatrudnienia. Jako przykład można wskazać takie grupy pracowników, jak: nauczyciele, straż graniczna, strażnicy gminni, członkowie korpusu służby cywilnej, pracownicy samorządowi, detektywi

4. DANE DOTYCZĄCE ZDROWIA

Dane dotyczące zdrowia to **wszystkie** dane o stanie zdrowia osoby, której dane dotyczą, **ujawniające informacje o przeszłym, obecnym lub przyszłym** stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą, w tym także informacje o korzystaniu przez daną osobę z usług opieki zdrowotnej, **niezależnie od źródła, z jakiego pochodzą.**

Przykłady danych dotyczących zdrowia:

- numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby fizycznej do celów zdrowotnych;
- informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych;
- informacje o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym, stanie fizjologicznym lub biomedycznym.

Źródłem danych może być np. lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne in vitro.

Dane osobowe zbierane są podczas rejestracji do usług zdrowotnych i podczas ich świadczenia.

Co do zasady przetwarzanie danych szczególnej kategorii jest zabronione. Niemniej jednak, RODO wprowadza wyjątki od tej zasady, co oznacza, że dane o stanie zdrowia mogą być przetwarzane np. gdy:
- osoba fizyczna wyrazi zgodę na przetwarzanie w jednym lub kilku konkretnych celach;
- przetwarzanie jest niezbędne dla profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego;
- przetwarzanie jest niezbędne ze względu na ochronę zdrowia publicznego, np. ochronę przed poważnymi transgranicznymi zagrożeniami zdrowotnymi, lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych.

Uwaga: przetwarzanie danych pacjenta w celu realizacji celów zdrowotnych **nie wymaga zgody pacjenta.**

Zgoda pacjenta wymagana jest w przypadku:

- przetwarzania danych do celów marketingowych (*marketingiem nie będzie przesyłanie zaproszeń na badania przesiewowe, zaproszeń na wykonanie szczepień, przekazywanie materiałów edukacyjnych, przekazywanie informacji o wydarzeniach prozdrowotnych);*

-przetwarzanie danych w związku z realizacją badań klinicznych lub badań naukowych

- przekazanie danych pacjenta do państwa trzeciego (w przypadku braku innych podstaw prawnych)

5. PRZETWARZANIE DANYCH OSOBOWYCH

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.

Przykłady operacji przetwarzania danych:

- zbieranie danych (np. przez papierowe formularze, przez stronę internetową);
- przeglądanie danych (np. na komputerze, w archiwum);
- ujawnienie danych (np. poprzez przesłanie e-maila, przesłanie listu wraz z danymi);
- porządkowanie danych (np. przypisywanie ich do różnych baz danych, porządkowanie danych w kartotekach)

Uwaga: Przeglądanie lub odczyt danych zawartych w dokumentacji medycznej pacjenta w celach dydaktycznych jest przetwarzaniem danych osobowych.

Przykładowe zbiory danych SP ZOZ w Sanoku w których przetwarza się dane osobowe:

- pacjenci i byli pacjenci
- potencjalni pracownicy i współpracownicy (kandydaci do pracy);
- pracownicy i współpracownicy, w tym byli pracownicy i współpracownicy oraz członkowie ich rodzin;

- dostawcy oraz ich pracownicy i współpracownicy (kontrahenci);
- dane z monitoringu wizyjnego;

Szpital przetwarza dane osobowe:

1) w formie tradycyjnej (dokumentacja papierowa) tj. dokumentacja medyczna, wyniki badań, akta osobowe pracowników, dokumenty wydrukowane zawierające dane osobowe.

Przykładowe czynności przetwarzania: wypełnienie dokumentacji medycznej, przechowywanie, przeglądanie, kopiowanie, organizowanie, udostępnianie, niszczenie.

2) w formie elektronicznej – (przetwarzane w systemach informatycznych)

Przykładowe czynności przetwarzania: wprowadzanie danych do systemu, zapisywanie, wyszukiwanie, kopiowanie, modyfikowanie, pobieranie, utrwalanie, organizowanie, usuwanie.

Wszystkie formy przetwarzania danych podlegają wymogom RODO.

6. ADMINISTRATOR DANYCH

Osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;

Administratorem danych Samodzielny Publiczny Zespół Opieki Zdrowotnej w Sanoku

Administratora danych reprezentuje Dyrektor Szpitala

Administrator danych ustala cele i sposoby przetwarzania danych osobowych, a także zobowiązany jest – uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia – wdrożyć odpowiednie środki techniczne i organizacyjne, by przetwarzanie danych osobowych odbywało się zgodnie z RODO.

7. PODMIOT PRZETWARZAJĄCY(PROCESOR)

Osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu i na rzecz administratora.

Procesorem będzie podmiot zewnętrzny, nie znajdujący się w strukturze organizacyjnej administratora, który zgodnie z zawartą z administratorem umową o powierzeniu danych do przetwarzania i tylko w zakresie w niej określonym wspiera administratora w określonych sferach jego działalności, przetwarzając w jego imieniu dane osobowe (np. firmy świadczące usługi

w zakresie opisywania badań radiologicznych, firmy zajmujące się niszczeniem dokumentów i sprzętu, firmy świadczące usługi z zakresu IT).

8. OSOBA UPOWAŻNIONA

Osoba upoważniona przez administratora do przetwarzania danych osobowych, nad którą administrator sprawuje bezpośrednią kontrolę w procesie przetwarzania danych realizowanym przez tę osobę np. pracownik, praktykant, stażysta, wolontariusz, zatrudniony na umowę cywilnoprawną.

9. INSPEKTOR OCHRONY DANYCH (IOD)

Osoba wyznaczona przez administratora danych lub podmiot przetwarzający, która monitoruje i weryfikuje przestrzeganie przepisów o ochronie danych osobowych oraz doradza w tym zakresie i wydaje odpowiednie rekomendacje.

Zadania IOD to:

- informowanie administratora, podmiotu przetwarzającego oraz pracowników o obowiązkach w zakresie ochrony danych osobowych wynikających z RODO,
- doradzanie, jak przestrzegać przepisów o ochronie danych osobowych,
- monitorowanie przestrzegania przepisów, polityk w zakresie ochrony danych osobowych,
- pomaganie przy sporządzaniu oceny ryzyka lub oceny skutków dla ochrony danych osobowych,
- zachowanie poufności względem wykonywanych zadań w ramach ochrony danych osobowych,
- pełnienie funkcji punktu kontaktowego dla organu nadzorczego.

IOD musi być niezwłocznie włączany we wszystkie sprawy organizacji dotyczące ochrony danych osobowych. IOD nie może otrzymywać od administratora ani podmiotu przetwarzającego dane instrukcji dotyczących wykonywania swoich zadań. IOD bezpośrednio podlega najwyższemu kierownictwu organizacji.

10. ORGAN NADZORCZY (art. 4 pkt. 21 RODO)

Niezależny organ publiczny ustanowiony przez państwo członkowskie UE odpowiedzialny za monitorowanie stosowania przepisów o ochronie danych osobowych.

W Polsce organem nadzorczym jest **Prezes Urzędu Ochrony Danych Osobowych** (PUODO)

11. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

Zgodnie z art. 5 ust. 1 RODO dane osobowe muszą być:

zasada legalności oraz przejrzystości	- przetwarzanie musi się odbywać zgodnie z prawem – przede wszystkim zgodnie z RODO, ale także polskimi przepisami np. ustawą o prawach pacjenta - przetwarzanie musi się odbywać w sposób rzetelny i przejrzysty tzn. zrozumiały dla pacjenta, pracownika lub innej osoby
zasada prawidłowości	- przetwarzane dane muszą być prawidłowe (prawdziwe i kompletne); - dane powinny być uaktualnione w przypadku stwierdzenia ich

	nieprawdziwości lub niekompletności; - dane nieprawidłowe powinny być niezwłocznie usunięte lub sprostowane; - nie można zbierać danych ze źródeł nieznanego pochodzenia.
zasada celowości	cel przetwarzania danych osobowych musi być z góry określony, a informacja ta musi zostać przekazana osobie, której dane dotyczą. Aby dane mogły być przetwarzane, musi istnieć konkretny, wyraźny i prawnie uzasadniony cel. Przetwarzanie danych w sposób niezgodny z ustalonymi celami jest zakazane
zasada adekwatności (minimalizacja danych)	przetwarzane mogą być tylko te dane osobowe, które są niezbędne do osiągnięcia celu przetwarzania. Nie wolno zbierać danych, które nie mają związku z celem przetwarzania, są nadmierne lub nieprzydatne(np. zgodnie z przepisami w dokumentacji dorosłego pacjenta mają się znaleźć następujące dane osobowe na jego temat: imię, nazwisko, data urodzenia, płeć, adres miejsca zamieszkania, numer PESEL. Dodatkowe zbieranie np. informacji o numerze buta lub o poglądach politycznych pacjenta będzie naruszeniem zasady minimalizacji danych)
zasada ograniczenia przechowywania	dane osobowe są przechowywane przez okres nie dłuższy, niż jest to niezbędne dla celów ich zebrania. W drodze wyjątku dane osobowe mogą być przechowywane przez dłuższy okres w celu archiwizacji w interesie publicznym lub dla celów badań naukowych bądź historycznych, pod warunkiem że zastosowano odpowiednie środki techniczne i organizacyjne (takie jak anonimizacja, szyfrowanie itd.).
zasada integralności i poufności	należy zapewnić, że przetwarzane dane nie zostały zmodyfikowane, usunięte, dodane czy zniszczone w sposób nieautoryzowany oraz zapobiegać sytuacjom, w których dane osobowe są udostępniane lub ujawniane nieuprawnionym podmiotom.

12. OBOWIĄZEK INFORMACYJNY(art. 13 i 14 RODO)

Obowiązkiem Administratora jest poinformowanie osoby, której dane dotyczą m.in. o:

- tożsamości i danych kontaktowych Administratora;
- danych kontaktowych Inspektora Ochrony Danych(jeżeli został powołany);
- celu przetwarzania danych osobowych;
- podstawie prawnej przetwarzania danych osobowych;
- przysługujących jej prawach;
- okresie przechowywania danych osobowych;
- odbiorcach danych osobowych lub o kategoriach odbiorców, jeśli istnieją;
- zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, gdy ma to zastosowanie;
- prawie wniesienia skargi do organu nadzorczego.

Obowiązek informacyjny ma na celu uświadomienie osoby, której dane dotyczą, o przysługujących jej prawach. Obowiązek ten realizowany jest najczęściej w postaci klauzul informacyjnych (komunikatów dotyczących przetwarzania danych) zamieszczanych w na stronach internetowych, tablicach ogłoszeń, dokumentacji wymagającej uzyskania zgody pacjenta.

13. DANE OSÓB ZMARŁYCH

RODO **nie ma zastosowania** do danych osobowych osób zmarłych, natomiast na podstawie art. 26 ust. 3b ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta, studenci

odbywający praktyki przygotowujący się do wykonywania zawodu medycznego zobowiązani są do zachowania w tajemnicy informacji zawartych w dokumentacji medycznej, także po śmierci pacjenta.

14. ZABEZPIECZENIE DANYCH OSOBOWYCH

RODO nie wskazuje konkretnych środków zabezpieczenia danych osobowych, jakie mają zostać wdrożone przez administratora lub podmiot przetwarzający lecz wprowadza tzw. *podejście oparte na ryzyku.*
RODO zawiera w art. 32 ust. 1 listę przykładowych środków technicznych i organizacyjnych, jednak, zgodnie z zasadą rozliczalności, to od administratora lub podmiotu przetwarzającego zależy wybór środków, jakie zostaną zastosowane (dobrane) adekwatnie do potrzeb wynikających z szacowania ryzyka.

Przykładowe środki to:

- pseudonimizacja i szyfrowanie danych osobowych;
- zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Istota podejścia opartego na ryzyku sprowadza się do tego, że każdy podmiot przetwarzający dane osobowe, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres i cele przetwarzania danych - samodzielnie decyduje, jakie konkretne środki zabezpieczenia danych wdrożyć, by zapewnić zgodność przetwarzania z wymaganiami RODO.
Przyjęcie tej zasady w RODO ma na celu zapewnienie ochrony przetwarzanych danych osobowych w sposób racjonalny, im większe ryzyko naruszenia praw i wolności – tym bardziej zaawansowane środki ochrony**.**

15. PSEUDONIMIZACJA I ANONIMIZACJA DANYCH OSOBOWYCH

Pseudonimizacja oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do identyfikowania osobie fizycznej. Jest to proces całkowicie odwracalny.

Anonimizacja – oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było przypisać konkretnej osobie, której dane dotyczą, za pomocą dodatkowych informacji lub wszelkich innych środków, jakimi dysponuje administrator lub podmiot przetwarzający. Zabieg ten ma charakter trwały i nieodwracalny, powodujący, że po jego przeprowadzeniu nie mamy do czynienia z danymi osobowymi. Dane zanonimizowane w taki sposób, że nie ma możliwości połączenia ich z konkretną osobą, są wyłączone z zakresu RODO.

16. STOSOWANIE TECHNICZNYCH I ORGANIZACYJNYCH ŚRODKÓW OCHRONY DANYCH OSOBOWYCH.

Techniczne i organizacyjne środki ochrony danych osobowych, to środki, które administrator lub podmiot przetwarzający dane stosuje w celu zapewnienia bezpieczeństwa danych osobowych, adekwatne do przeprowadzonej oceny ryzyka przetwarzania danych osobowych.

Przykładowe **środki organizacyjne** stosowane w Szpitalu:

- wdrożone polityki ochrony danych, procedury, instrukcje, regulaminy;
- upoważnienia do przetwarzania danych osobowych;
- oświadczenia o zachowaniu poufności;
- szkolenia dla osób przetwarzających dane osobowe;

Przykładowe **środki techniczne** stosowane w Szpitalu:

- monitoring wizyjny;
- przechowywanie danych osobowych formie papierowej w zamykanych szafkach, szafach lub szufladach;
- stosowanie oprogramowania antywirusowego;
- stosowanie systemu kopii zapasowych;
- stosowanie loginu i hasła (systemu uwierzytelniania)
- stosowanie systemów zasilania bezprzerwowego (UPS);

17. INCYDENT BEZPIECZEŃSTWA

Pojedyncze zdarzenie lub seria niepożądanych albo niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji. Incydentem bezpieczeństwa jest każde zdarzenie, którego skutkiem jest:

- zniszczenie;
- utrata;
- modyfikacja;
- nieuprawnione ujawnienie;
- nieuprawniony dostęp innego podmiotu do danych osobowych, które przedsiębiorca przesyła, przechowuje lub w inny sposób przetwarza

Można wyróżnić trzy zasadnicze grupy incydentów w ochronie danych osobowych:

umyślne incydenty

(np. kradzież danych i sprzętu, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie danych, włamanie do systemu informatycznego lub pomieszczeń)

zdarzenia losowe wewnętrzne

(np. awaria komputera/serwera/dysku twardego/oprogramowania, pomyłki informatyków, utrata danych)

zdarzenia losowe zewnętrzne

(np. pożar, zalanie wodą, utrata zasilania, utrata łączności)

Incydent bezpieczeństwa może doprowadzić do naruszenia danych osobowych.

Przykłady incydentów

- kradzież lub zgubienie nośników danych takich jak: smartfony, laptopy, przenośne dyski,teczki z papierowymi dokumentami;
- niszczenie dokumentów w wersji papierowej poprzez ich ręczne pogięcie, podarcie i wyrzucenie do kosza na śmieci. Takie dokumenty można łatwo odzyskać. W celu prawidłowego usunięcia danych osobowych, należy skorzystać z niszczarki. W przypadku elektronicznych nośników należy skorzystać ze specjalistycznego oprogramowania do usuwania danych (nie wystarczy tylko same formatowanie);
- obecność w budynku lub pomieszczeniach, w których przetwarzane są dane osobowe osób nieuprawnionych;
- otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe;
- aktywne konta systemowe i mailowe byłych pracowników, którym powinien być już dawno odebrany dostęp, a który nie raz przydzielany był bezterminowo;
- niewylogowywanie się przed opuszczeniem stanowiska pracy;
- pozostawienie wydruków na drukarce, ksero;
- niewykonywanie w określonym terminie kopii bezpieczeństwa oraz nie sprawdzanie możliwości jej odtworzenia;
- ustawienie ekranów monitorów pozwalające na wgląd do danych osobowych osobom postronnym (sam wgląd jest już przetwarzaniem);
- wynoszenie danych osobowych na zewnątrz organizacji w formie papierowej lub elektronicznej bez upoważnienia;
- udostępnianie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej;
- telefoniczne próby wyłudzania danych osobowych bez właściwej weryfikacji rozmówcy;
- nieaktualizowanie oprogramowania lub błędna konfiguracja systemu – wykorzystanie ujawnionej podatności;
- uniemożliwienie prawidłowego działania systemów lub usług sieciowych poprzez zajęcie wszystkich dostępnych zasobów;
- emaile zachęcające do ujawnienia identyfikatora lub hasła do systemu/programu/bankowości;
- pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;
- przechowywanie haseł do systemu/programów w pobliżu komputera;

- podszywanie się hakerów pod znane firmy wysyłające wiadomości zawierające złośliwe załączniki, które po kliknięciu w załącznik lub link szyfrują dane w taki sposób, że nie można uzyskać dostępu do nich bez użycia klucza, który należy odkupić od hakerów (lub przywrócić kopie bezpieczeństwa).

18. NARUSZENIE OCHRONY DANYCH OSOBOWYCH

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.

Aby doszło do naruszenia ochrony danych osobowych, konkretny incydent bezpieczeństwa musi doprowadzić do przynajmniej jednego z poniższych skutków:

- utraty poufności danych osobowych
- utraty integralności danych osobowych
- utraty dostępności danych osobowych

Naruszenie poufności polega na ujawnieniu danych osobowej nieuprawnionej osobie.
Naruszenie dostępności polega na czasowej bądź trwałej utracie lub zniszczeniu danych osobowych.
Naruszenie integralności polega na zmianie treści danych osobowych w sposób nieautoryzowany.

Gdy do dojdzie do naruszenia i prawdopodobnie naruszenie to stwarza ryzyko dla praw i wolności osób fizycznych tj. może nieść za sobą istotne negatywne skutki dla osoby, której dane zostały naruszone (np. popełnienie przestępstwa na jej szkodę, kradzież tożsamości, naruszenie dobrego imienia itd.)., Szpital powinien **zgłosić takie naruszenie organowi nadzorczemu bez zbędnej zwłoki, nie później niż w terminie 72 godzin od stwierdzenia naruszenia.**

Jeżeli może ono powodować **wysokie ryzyko dla osób poszkodowanych**, także muszą one zostać powiadomione (chyba że wdrożono skuteczne środki techniczne i organizacyjne w zakresie ochrony lub inne środki gwarantujące, że ryzyko już raczej nie wystąpi).

Przykłady sytuacji, w których będzie występowała konieczności poinformowania osób o naruszeniu:

- niedostępność przez 30 godzin szpitalnej dokumentacji medycznej w wyniku cyberataku,

- cyberatak i publikacja w Internecie identyfikatorów użytkownika, haseł i historii zakupów klientów platformy internetowej

RODO przewiduje 3 przypadki w których Administrator nie musi powiadamiać osób o naruszeniu:

1) **administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony** i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym, np. dane osobowe zostały zabezpieczone za pomocą szyfrowania lub tokenizacji,

2) **administrator natychmiast po wystąpieniu naruszenia podjął środki eliminujące prawdopodobieństwo wysokiego ryzyka** naruszenia praw lub wolności osoby, np. zorientował się on, że przesyłka, w której znajdowały się dane osobowe została zaadresowana do niewłaściwego nadawcy i

podjął on natychmiast kroki w celu skontaktowania się z kurierem aby nie dopuścić do dostarczenia przesyłki,

3) **kontakt z osobami wymagałby niewspółmiernie dużego wysiłku**, z zastrzeżeniem, że takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób, np. dokumenty, w których znajdowały się dane osobowe uległy zniszczeniu i administrator danych osobowych nie ma możliwości kontaktu bezpośredniego z osobami, których dane dotyczą, więc zasadnym będzie w tej sytuacji wydanie publicznego komunikatu.

Przykładami naruszeń w Szpitalu:
- umożliwienie wglądu do dokumentacji medycznej osobom nieuprawnionym

Zabroniony jest wgląd do dokumentacji medycznej pacjentów Szpitala przez osoby, które nie są do tego uprawnione na podstawie obowiązujących przepisów prawa.

- udostępnienie dokumentacji medycznej lub informacji o stanie zdrowia osobom nieuprawnionym

Zabronione jest udostępnianie dokumentacji medycznej i informacji o pacjentach (danych osobowych pacjentów) osobom i podmiotom nieuprawnionym, niezgodnie z ustawą o prawach pacjenta i Rzeczniku Praw Pacjenta.

- pozostawienie dokumentów zawierających dane osobowe, w tym dokumentacji medycznej w miejscach bez nadzoru

Dokumenty zawierające dane osobowe pacjentów powinny być zabezpieczone w sposób uniemożliwiający zapoznanie się z tymi danymi przez osoby nieuprawnione.
Dokumenty, z których aktualnie nie korzystamy należy przechowywać w zamkniętych szafach, biurkach itp., obowiązuje zasada „czystego biurka".

19. POSTĘPOWANIE W PRZYPADKU PODEJRZENIA NARUSZENIA OCHRONY DANYCH OSOBOWYCH

W przypadku podejrzenia naruszenia ochrony danych osobowych należy:

- niezwłocznie zgłosić Inspektorowi ochrony danych podejrzenie/stwierdzenie naruszenia ochrony danych osobowych.
- powstrzymać się od wszelkich działań mogących utrudnić ustalenie okoliczności naruszenia, jednakże np. w przypadku znalezienia na terenie Szpitala niezabezpieczonych dokumentów zawierających dane osobowe, w tym dokumentacji medycznej, jak również jej kopii, wydruków, itp., należy je zabezpieczyć, aby informacje zawarte w dokumentacji nie zostały ujawnione osobom nieuprawnionym.
- współpracować z IOD w celu wyjaśnienia wszystkich okoliczności naruszenia ochrony danych osobowych.

W zgłoszeniu podejrzenia/stwierdzenia naruszenia należy wskazać:

- datę, godzinę zdarzenia;

- miejsce wystąpienia incydentu;
- opis zaistniałego incydentu;
- wskazać przyczynę lub potencjalną przyczynę wystąpienia incydentu/naruszenia;
- ustalić możliwe skutki wynikające z naruszenia;
- opisać dotychczasowe działania w związku z incydentem;
- wskazać znane danej osobie sposoby zabezpieczenia danych osobowych.

20. ODPOWIEDZIALNOŚĆ KARNA ZA NARUSZENIE PRZEPISÓW O OCHRONIE DANYCH OSOBOWYCH

Wobec wszystkich osób uczestniczących w przetwarzaniu danych osobowych mają zastosowanie przepisy o odpowiedzialności karnej za naruszenie przepisów o ochronie danych osobowych (nielegalne przetwarzanie danych osobowych).

Brzmienie art. 107 ust. 1 i 2 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych:

„*1. Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.*
2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech”.

Osoby naruszające zasady bezpieczeństwa danych osobowych, w tym Studenci odbywający praktyki, mogą ponosić sankcje karne na podstawie przepisów o ochronie danych osobowych.
Osoby niebędące pracownikami Szpitala, w tym Studenci odbywający praktyki , ponoszą wobec Szpitala odpowiedzialność odszkodowawczą na zasadach określonych w kodeksie cywilnym.

21. PODSTAWOWE OBOWIĄZKI STUDENTÓW ODBYWAJĄCYCH PRAKTYKI

Studenci odbywający praktyki mogą przebywać w pomieszczeniach, w których przetwarzane są dane osobowe, wyłącznie w obecności Personelu Szpitala.
Studenci odbywający praktyki są zobowiązani w szczególności do zapoznania się z:

- ogólnie obowiązującymi przepisami prawa w zakresie ochrony danych osobowych, w szczególności z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 2016/679 z 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 95/45/WE (ogólne rozporządzenie o ochronie danych osobowych) oraz z ustawą z dnia 10 maja 2018 roku o ochronie danych osobowych;
- regulacjami wewnętrznymi Szpitala wskazanymi przez opiekuna grupy, w szczególności z zakresu ochrony danych osobowych, dokumentacji medycznej oraz bezpieczeństwa informacji

Studenci odbywający praktyki są zobowiązani w szczególności do przestrzegania zasad ochrony danych osobowych obowiązujących w Szpitalu wynikających z przepisów prawa i regulacji wewnętrznych, w tym:

- zachowania należytej staranności w celu ochrony danych osobowych;
- zapewnienia bezpieczeństwa przetwarzania danych osobowych, w szczególności poprzez ich ochronę przed nieuprawnionym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem, w tym stosowanie wymaganych środków technicznych i organizacyjnych zapewniających ochronę danych osobowych;
- zachowania w tajemnicy danych osobowych uzyskanych w związku z uczestnictwem w zajęciach na terenie Szpitala (bez względu na sposób ich uzyskania – pisemny, elektroniczny, ustny), zarówno w trakcie odbywania zajęć jak również po ich zakończeniu. Zobowiązanie do zachowania tajemnicy danych dotyczących pacjenta ma zastosowanie również po śmierci pacjenta;
- przeciwdziałania naruszeniom ochrony danych osobowych oraz zgłaszanie przypadków naruszenia lub podejrzenia naruszenia ochrony danych.