Zarządzenie nr 67/2018
Rektora Uniwersytetu Medycznego w Białymstoku
z dnia 5 listopada 2018
w sprawie wprowadzenia zasad szacowania ryzyka w ochronie danych osobowych
w Uniwersytecie Medycznym w Białymstoku

Na podstawie art. 24, 25, 32 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016) zwanego dalej „RODO" zarządzam, co następuje:

§1

1. Wprowadzam zasady szacowania ryzyka w ochronie danych osobowych w Uniwersytecie Medycznym w Białymstoku.
2. Właściciele procesów przetwarzania, w szczególności kierownicy jednostek organizacyjnych administracji, kierownicy zadań w projektach, przetwarzający dane osobowe dokonują szacowania ryzyka w obszarze przetwarzania danych osobowych.
3. Szacowania ryzyka w ochronie danych osobowych dokonuje się nie rzadziej niż raz w roku.

§2

Niniejsze zasady opisują sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

§3

1. Definicje:
   1) aktywa – to zasoby wykorzystywane przez Uniwersytet Medyczny w Białymstoku do przetwarzania danych osobowych,
   2) naruszenie (incydent) ochrony danych osobowych - to 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,
   3) zagrożenie - potencjalne naruszenie (potencjalny incydent),
   4) prawdopodobieństwo – to szansa na wystąpienie zagrożenia,
   5) ryzyko - prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie zasobów,
   6) skutek – niepożądany wpływ na przetwarzane dane oraz prawa i wolności osób, których dane dotyczą,
   7) zabezpieczenie – to środek, który modyfikuje ryzyko naruszenia bezpieczeństwa,

8) poufność danych – właściwość zapewniająca niedostępność danych dla osób/podmiotów nieuprawnionych,
9) integralność danych – właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w nieautoryzowany sposób,
10) dostępność danych - oznacza niczym nieograniczoną możliwość korzystania z danych przez uprawnione osoby.

2. Cel szacowania ryzyka:
   1) szacowanie ryzyka przeprowadza się w celu oceny ryzyka dla przetwarzanych danych osobowych i zabezpieczeniu danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych,
   2) ocenę ryzyka przeprowadza się w oparciu o poufność, integralność i dostępność danych,
   3) oceniając ryzyko w zakresie bezpieczeństwa danych, należy wziąć pod uwagę ryzyko związane z przetwarzaniem danych osobowych – takie jak przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych – i mogące w szczególności prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych,
   4) wynik analizy ryzyka wskazuje jakie zastosować środki fizyczne, informatyczne i organizacyjne aby zminimalizować ryzyko i zapewnić odpowiedni stopień bezpieczeństwa odpowiadający ryzyku. Środki takie powinny zapewnić odpowiedni poziom bezpieczeństwa, oraz uwzględniać stan wiedzy technicznej oraz koszty ich wdrożenia w stosunku do ryzyka i charakteru danych osobowych podlegających ochronie. Odpowiedni stopień bezpieczeństwa daje gwarancję, że podstawowe prawa i wolności osób fizycznych, których dane przetwarzamy są właściwie chronione,
   5) szacowania ryzyka dokonuje się w stosunku do operacji (czynności przetwarzania) np. rekrutacja pracowników, rekrutacja studentów, udzielanie pomocy materialnej studentom, ubieganie się o środki z ZFŚS itp. lub w odniesieniu do zbiorów danych np. zbiór danych studentów, doktorantów itp.,
   6) szacowanie ryzyka jest procesem cyklicznym i ciągłym.

3. Metoda analizy ryzyka

Metodę analizy ryzyka przedstawia poniższa tabela:

Rodzaj operacji przetwarzania danych lub zbioru danych	Aktywa (zasoby) załącznik nr 1	Stosowane zabezpieczenia załącznik nr 5	Zidentyfikowane zagrożenie załącznik nr 2	Skutek wystąpienia naruszenia (S) załącznik nr 4	Prawdopodobieństwo (P) (od 1 do 4) załącznik nr 3	Poziom ryzyka zgodnie z mapą ryzyka (R) R = P * S załącznik nr 6 (od 1 do 16 - od niskiego do wysokiego)

1) ryzyko w Uczelni szacujemy biorąc pod uwagę aktywa (zasoby) podlegające ochronie oraz zagrożenia dla utraty poufności, integralności i dostępności tych zasobów,
2) katalog aktywów (zasobów) stanowi załącznik nr 1 do zarządzenia,
3) katalog potencjalnych zagrożeń stanowi załącznik nr 2 do zarządzenia,
4) katalog zabezpieczeń stanowi załącznik nr 5 do zarządzenia ,
5) prawdopodobieństwo i powagę ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, należy określić poprzez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych,
6) ryzyko należy oszacować na podstawie obiektywnej oceny, w ramach której stwierdza się, czy z operacjami przetwarzania danych wiąże się bardzo wysokie, wysokie, średnie czy niskie ryzyko,
7) oceniając ryzyko należy uwzględnić:
    a) rodzaj danych (dane zwykłe lub szczególnych kategorii tzw. wrażliwe),
    b) skalę przetwarzanych danych (duże zasoby, małe zasoby),
    c) korzystanie z usług podwykonawców,
    d) przekazywanie danych do państw trzecich.

   Przetwarzanie danych szczególnych kategorii w dużych zasobach i przekazywanie danych do państw trzecich znacznie podwyższa stopień ryzyka.
8) oceniając ryzyko należy przeanalizować czy naruszenia praw lub wolności osób, o różnym prawdopodobieństwie i wadze zagrożeń, może wynikać z przetwarzania danych osobowych mogącego prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, w szczególności: jeżeli przetwarzanie może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną,
9) wyliczenie ryzyka dla zagrożeń polega na:
    a) określeniu Prawdopodobieństwa (P) wystąpienia poszczególnych zagrożeń w zbiorze lub w procesie przetwarzania. Skalę prawdopodobieństwa wystąpienia zagrożenia określa załącznik nr 3 do zarządzenia ,
    b) określeniu Skutków (S) wystąpienia naruszenia, uwzględniając straty finansowe, utratę reputacji, sankcje/skutki karne. Poziom i opis możliwych skutków stanowi załącznik nr 4 do zarządzenia,
    c) wyliczeniu poziomu Ryzyka (R) zgodnie z mapą ryzyka dla wszystkich zagrożeń i ich skutków w/g formuły: R = P * S. Mapa ryzyka stanowi załącznik nr 6 do zarządzenia,
10) dalsze postępowanie z ryzykiem:

    Jeśli poziom ryzyka określony został jako wysoki lub bardzo wysoki należy stworzyć plan postępowania z ryzykiem – określić środki zabezpieczające. Wzór planu postępowania z ryzykiem stanowi załącznik nr 7 do zarządzenia.

    W celu obniżenia poziomu ryzyka można przeprowadzić następujące czynności:
    - unikanie ryzyka – eliminacja działań powodujących ryzyko np. poprzez modyfikację procedur, które mają na celu wyeliminowanie potencjalnie niebezpiecznych sytuacji,

- obniżanie ryzyka - zastosowanie zabezpieczeń w celu obniżenia ryzyka,
- przeniesienie ryzyka np. poprzez powierzenie procesów przetwarzania podmiotom zewnętrznym.

4. Ponowna analiza ryzyka przeprowadzana jest cyklicznie, co najmniej raz w roku lub po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie nowych zbiorów/kategorii osób, realizacja nowych procesów przetwarzania, zmiany prawne).

§4

Zarządzenie wchodzi w życie z dniem podpisania.

Rektor

prof. dr hab. Adam Krętowski

Załącznik nr 1 do Zarządzenia nr 67 /2018 z dnia 5.11.2018r.

KATALOG AKTYWÓW - zasobów

INFORMACJE
dane osobowe
dane dostępowe (loginy, hasła, piny)
dane dotyczące zabezpieczeń (klucze szyfrujące, certyfikaty)
logi systemowe
dokumentacja techniczna
polityki bezpieczeństwa
procedury odtworzeniowe
umowy

PROGRAMY I SYSTEMY OPERACYJNE - OPROGRAMOWANIE
systemy operacyjne
oprogramowanie użytkowe – np. pakiety biurowe
serwery usługowe (www, poczta, serwery plików, bazy danych
oprogramowanie administracyjne (inwentaryzacja, monitoring, backup)
sterowniki
oprogramowanie układowe (firmware)
strony www i aplikacje webowe
oprogramowanie rozwijane we własnym zakresie

SPRZĘT
serwery
stacje robocze
laptopy
monitory
tablety
smartfony
drukarki
skanery
niszczarki

TELEKOMUNIKACJA
centrale telefoniczne
centrale voip
urządzenia klienckie (telefony, faxy, modemy)
łącza (np. Internet)

NOŚNIKI DANYCH
elektroniczne nośniki z danymi np. pendrive
dokumentacja papierowa

SIEĆ
usługi sieciowe
okablowanie
urządzenia aktywne (np. switche, routery)
systemy sieciowe (np. firewalle, proxy)

INFRASTRUKTURA – OBSZARY CHRONIONE
serwerownie
punkty dystrybucyjne sieci
punkty składowania i przetwarzania danych (elektronicznych i papierowych)
kanały telekomunikacyjne
rozdzielnie elektryczne
stanowiska monitoringu

SPRZĘT WSPOMAGAJĄCY
klimatyzatory
zasilacze awaryjne i agregaty
monitoring środowiskowy (czujki temp., zalania, dymu)
systemy automatycznego gaszenia
monitoring wizyjny (kamery, rejestratory)
systemy alarmowe
systemy kontroli dostępu

PRACOWNICY I WSPÓŁPRACOWNICY - PERSONEL
kompetencje
doświadczenie
know-how

DOSTAWCY
oprogramowania
usług chmurowych
usług internetowych (hosting, dns, poczta)
łączy
usług serwisowych i gwarancyjnych
wsparcia technicznego
personelu

Załącznik nr 2 do Zarządzenia nr 67 /2018 z dnia 5.11.2018r.

KATALOG POTENCJALNYCH ZAGROŻEŃ

ZNISZCZENIA FIZYCZNE
Pożar
Zalanie
Zanieczyszczenie
Poważny wypadek
Katastrofa budowlana
Zniszczenie urządzeń lub nośników
Wybuch bomby, ładunku wybuchowego
Pył, korozja, wychłodzenie

ZJAWISKA NATURALNE
Zjawiska klimatyczne – wyładowania atmosferyczne
Zjawiska klimatyczne – wichury, nawałnice
Zjawiska klimatyczne – upały
Zjawiska klimatyczne – niskie temperatury
Powódź

UTRATA PODSTAWOWYCH USŁUG
Awaria systemu klimatyzacji lub dostawy wody
Awaria dostawy prądu

NARUSZENIE BEZPIECZEŃSTWA INFORMACJI
Wykorzystanie oprogramowania szpiegującego
Szpiegostwo, podsłuch
Terroryzm
Wandalizm
Kradzież nośników, dokumentów, urządzenia
Zagubienie urządzeń, nośników lub dokumentów
Wykorzystanie źle zniszczonych nośników
Ujawnienie
Nieuprawniony dostęp/wgląd
Nieuprawnione kopiowanie danych
Manipulowanie urządzeniem
Sfałszowanie oprogramowania

AWARIE TECHNICZNE
Awaria urządzenia
Niewłaściwe funkcjonowanie urządzeń
Niewłaściwe funkcjonowanie oprogramowania

NIEAUTORYZOWANE DZIAŁANIA
Nieautoryzowane użycie urządzeń
Nieuprawnione kopiowanie oprogramowania
Użycie fałszywego programu, aplikacji
Zniekształcenie danych
Nielegalne przetwarzanie danych

NARUSZENIE BEZPIECZEŃSTWA FUNKCJI
Błąd użytkownika
Naruszenie praw
Fałszowanie praw
Odmowa działania
Naruszenie dostępności personelu
Choroba ważnych osób

INNE
nieznajomość przepisów o ochronie danych osobowych
brak procedur
nieprzestrzeganie procedur przez pracowników
brak wymuszania zmiany haseł
brak haseł
łatwe, standardowe hasła
brak wygaszaczy ekranu

Załącznik nr 3 do Zarządzenia nr 67/2018 z dnia 5.11.2018r.

SKALA PRAWDOPODOBIEŃSTWA WYSTĄPIENIA ZAGROŻENIA

PRAWDOPODOBIEŃSTWO	POZIOM	OPIS
BARDZO WYSOKIE	4	Zdarzenie prawie pewne
WYSOKIE	3	Zdarzenie możliwe
ŚREDNIE	2	Zdarzenie raczej nie wystąpi
NISKIE	1	Zdarzenie prawie niemożliwe

Załącznik nr 4 do Zarządzenia nr 67/2018 z dnia 5.11.2018r.

OKREŚLENIE POZIOMU I OPIS SKUTKÓW

SKUTEK	POZIOM	OPIS
BARDZO WYSOKI	4	Zagrożenie dla kontynuacji działania, drastycznie zakłóca lub uniemożliwia pracę Poważna odpowiedzialność prawna Poważna odpowiedzialność finansowa, w tym kary pieniężne Negatywny rozgłos medialny na skalę krajową Istotne lub nieodwracalne konsekwencje dla osób, których dane dotyczą
WYSOKI	3	Może zakłócić znacząco pracę, mając poważny wpływ na działanie Możliwa jest odpowiedzialność prawna Średnia odpowiedzialność finansowa, w tym kary pieniężne Negatywny rozgłos medialny na skalę lokalną Istotne konsekwencje dla osób, których dane dotyczą ale możliwe do rozwiązania z wieloma trudnościami
ŚREDNI	2	Krótkotrwały, poważny wpływ na działanie, może zakłócić pracę, ale można przywrócić pracę łatwo dostępnymi środkami Niewielka odpowiedzialność finansowa, raczej nie występują kary finansowe lub występują bardzo niskie Niewielkie konsekwencje dla osób, których dane dotyczą i możliwe do rozwiązania w łatwy sposób
NISKI	1	Brak poważnego wpływu na działanie, zadania mogą być nadal realizowane Osoby, których dane dotyczą nie odczuwają skutków

Załącznik nr 5 do Zarządzenia nr 67/2018 z dnia 5.11.2018r.

KATALOG ZABEZPIECZEŃ

Zabezpieczenia organizacyjne i prawne:

Regulacje wewnętrzne

Polityka ochrony danych osobowych, Instrukcja zarządzania systemem informatycznym i inne.
Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy. Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych i podpisują stosowne Oświadczenie poufności.

Zapoznawanie pracowników z zasadami ochrony danych

Szkolenia wewnętrzne, informacje na stronie internetowej, wysyłanie informacji drogą mailową, indywidualne spotkania.

Umowy

Umowy powierzenia.

Procedury napraw w serwisach zewnętrznych: zawarte w Instrukcji zarządzania systemem informatycznym.

Audyty

Audyty wykonywane przez Inspektora Ochrony Danych w jednostkach organizacyjnych Uczelni.

Testy penetracyjne

Wykonywanie testów w celu wykrycia słabości np. poprzez kontrolowane ataki.

Procedury przywracania w razie incydentu

Plan ciągłości działania opisany w Instrukcji zarządzania systemem informatycznym.

Zabezpieczenia fizyczne

Polityka kluczy

Uregulowana Zarządzeniem Rektora w sprawie zasad postępowania z kluczami do pomieszczeń w budynkach w Uniwersytecie Medycznym w Białymstoku, w szczególności w zakresie kontroli kluczy zapasowych, zakazu wstępu osobom nieupoważnionym, kontroli wydawania kluczy, kontroli składowania kluczy.

Dostęp do sprzętu

Ograniczenie dostępu do komputerów, drukarek, ksero osobom nieupoważnionym, chyba że w obecności osoby upoważnionej.

Zabezpieczenie dostępu do pomieszczeń biurowych i archiwum

Ograniczenie dostępu: drzwi zamykane na klucz.

Zabezpieczenie dostępu do serwerowni: drzwi zamykane na klucz, wejście kodowane.

Zabezpieczenie dokumentacji w pomieszczeniach: zamknięte niemetalowe szafy, zamknięte metalowe szafy, biurka zamykane na klucz, sejf, skrytki na klucze.

Systemy alarmowe / zabezpieczenia antywłamaniowe: system alarmowy, kraty, rolety.

Ochrona fizyczna obiektu / pomieszczeń: ochrona własna, firma ochroniarska.

Strefy dostępu: Organizacja stref ograniczonego dostępu.

Zabezpieczenia techniczne

System kontroli dostępu: System kart wejściowych, portiernia.

System ppoż: system w obiekcie, system gaszenia serwerowni, gaśnice.

Monitoring środowiskowy: w archiwum – higrometry, czujnik obecności wody, osuszacz powietrza; w serwerowni - czujnik temperaturowy, powiadamianie mailem o alertach.

Klimatyzacja: klimatyzacja w serwerowni.

Monitoring wizyjny: monitoring wizyjny w obrębie obiektu i otoczeniu.

Systemy UPS / agregaty prądotwórcze: Zastosowano UPS podtrzymujący zasilanie serwera, UPS na kluczowych elementów systemu IT.

Zabezpieczenia informatyczne

- systemy antywirusowy i antyspamowy,
- sewery proxy i bramki filtrujące,
- systemy firewall,
- szyfrowanie,
- aktualizacje systemu,
- backupy i archiwizacja,
- rozliczalnosć operacji,
- postępowanie z nośnikami,
- zabezpieczenie pracy użytkowników: Procedura korzystania z internetu, Procedura korzystania z poczty elektronicznej, zabezpieczenia: zahasłowane wygaszacze ekranu aktywowane w przypadku nieaktywności użytkownika, poufne ustawienie monitorów,
- niszczenie nośników: niszczarki,
- zarządzanie uprawnieniami: Procedura zarządzania uprawnieniami,
- uwierzytelnianie: Polityka haseł, zabezpieczenia: długość hasła, częstotliwość zmiany, wymuszenie zmiany,
- przesyłanie danych osobowych szczególnych kategorii pocztą elektroniczną poza Uczelnię w postaci zaszyfrowanej (kod odszyfrowujący powinien być przekazany oddzielnie),
- zabezpieczone nośniki danych (laptopy, pendrive) z danymi osobowymi wynoszone poza Uczelnię np. zaszyfrowane.

Załącznik nr 6 do Zarządzenia nr 67/2018 z dnia 5.11.2018r.

MAPA RYZYKA

Wartość ryzyka (R)

Prawdopodobieństwo wystąpienia (P)

Skutek (S)

R= P*S

			Skutek			
			Niski (N)	Średni (Ś)	Wysoki (W)	Bardzo wysoki (BW)
			1	**2**	**3**	**4**
Prawdopodobieństwo	Niskie (N)	**1**	N	N	Ś	W
	Średnie (Ś)	**2**	N	Ś	Ś	W
	Wysokie (W)	**3**	Ś	Ś	W	BW
	Bardzo wysokie (BW)	**4**	Ś	W	BW	BW

Ryzyko niskie – akceptujemy

Ryzyko średnie – możemy zaakceptować lub obniżyć

Ryzyko wysokie i bardzo wysokie – nie akceptujemy, obniżamy

Załącznik nr 7 do Zarządzenia nr 67/2018 z dnia 5.11.2018r.

PLAN POSTĘPOWANIA Z RYZYKIEM

Zagrożenie (ryzyko do obniżenia)	Określenie działań - zabezpieczenie do wdrożenia	Osoba odpowiedzialna za realizację planu	Termin zrealizowania planu