SZPITAL UNIWERSYTECKI
W KRAKOWIE

Podstawowe zasady związane z bezpieczeństwem informacji obowiązujące Dostawców (Wykonawców) na terenie Szpitala Uniwersyteckiego w Krakowie

Przedstawione poniżej zasady wynikają z wymagań 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) („RODO"), ustawy z dnia 5 lipca 2018 r. krajowym systemie cyberbezpieczeństwa oraz aktów wewnętrznych Szpitala Uniwersyteckiego dotyczących bezpieczeństwa informacji.

1. Definicje i terminologia:

1.1. **Bezpieczeństwo informacji** - zapewnienie poufności, integralności i dostępności informacji, przy zachowaniu autentyczności, niezaprzeczalności i rozliczalności działań, zgodnie z obowiązującymi w Szpitalu wymaganiami, przy czym w/w terminy mają następujące znaczenie:

- ***poufność informacji*** – informacje nie są udostępniane nieupoważnionym podmiotom;
- ***integralność informacji*** – informacje nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
- ***dostępność informacji*** – osoby upoważnione mają dostęp do informacji, gdy istnieje taka potrzeba;
- ***autentyczność*** – pochodzenie lub zawartość informacji jest taka, jak deklarowana;
- ***niezaprzeczalność*** – brak jest możliwości zanegowania swego uczestnictwa w całości lub w części wymiany informacji przez jeden z podmiotów uczestniczących w tej wymianie;
- ***rozliczalność*** – działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

1.2. **Cyberbezpieczeństwo** - odporność Systemów Informatycznych wraz z przetwarzanymi w nich danymi w postaci elektronicznej na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

1.3. **Incydent bezpieczeństwa** - zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo informacji.

1.4. **Incydent cyberbezpieczeństwa** - zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo.

1.5. **Inspektor Ochrony Danych** – osoba nadzorująca przestrzeganie zasad ochrony danych osobowych w Szpitalu.

1.6. **Naruszenie ochrony danych osobowych** - 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.

1.7. **Pełnomocnik Dyrektora ds. Cyberbezpieczeństwa** – osoba odpowiedzialna za zapewnienie odpowiedniego poziomu cyberbezpieczeństwa w Szpitalu.

2. Zasady związane z bezpieczeństwem informacji obowiązujące Dostawców (Wykonawców) współpracujących ze Szpitalem Uniwersyteckim.

2.1. Dostawcy (Wykonawcy) zobowiązują się **akceptować i stosować wszystkie obowiązujące w Szpitalu Uniwersyteckim zasady związane z bezpieczeństwem informacji**, w tym bezpieczeństwem danych osobowych oraz cyberbezpieczeństwem dotyczącym systemów informacyjnych wykorzystywanych do świadczenia usługi kluczowej - odpowiednio do rodzaju i zakresu przyznanego im dostępu do zasobów informacyjnych.

2.2. Dostawcy (Wykonawcy) **odpowiedzialni są w szczególności za**:

a) **zapoznanie się z przepisami prawa** w zakresie bezpieczeństwa informacji, w szczególności z przepisami dotyczącymi ochrony danych osobowych (w tym RODO) oraz cyberbezpieczeństwa;

b) **niewykorzystywanie informacji do celów innych niż realizacja umowy zawartej ze Szpitalem Uniwersyteckim;**

c) zapewnienie, że osoby przez niego upoważnione będą mogły uzyskać dostęp do informacji wyłącznie w zakresie niezbędnym ze względu na ich udział w realizacji umowy zawartej ze Szpitalem Uniwersyteckim;

d) **zapewnienie bezpieczeństwa informacji,** w tym przetwarzanych danych osobowych m.in. poprzez ich zabezpieczenie przed naruszeniem ochrony danych osobowych oraz incydentami cyberbezpieczeństwa;

e) **zachowanie w tajemnicy wszelkich informacji**, a w szczególności danych osobowych oraz wiedzy o zabezpieczeniach organizacyjnych, technicznych i infrastrukturze Szpitala, uzyskanych w związku z realizacją umowy zawartej ze Szpitalem Uniwersyteckim;

f) **stosowanie środków technicznych i organizacyjnych** zapewniających ochronę informacji, w tym danych osobowych;

g) **zgłaszanie Inspektorowi Ochrony Danych lub Pełnomocnikowi Dyrektora ds. Cyberbezpieczeństwa** każdego zauważonego przypadku naruszenia bezpieczeństwa informacji:

Rodzaj incydentu	**Naruszenie ochrony danych osobowych / podejrzenie takiego naruszenia**	**Negatywne zdarzenia związane z cyberbezpieczeństwem, które mogą stanowić incydent cyberbezpieczeństwa**
Kogo należy powiadomić	Inspektor Ochrony Danych tel. 12 424 7828, e-mail: dane.osobowe@su.krakow.pl	Pełnomocnik Dyrektora ds. Cyberbezpieczeństwa tel. 12 400 1280, e-mail: cyberbezpieczenstwo@su.krakow.pl
Forma powiadomienia	za pośrednictwem systemu Helpdesk, a w przypadku braku dostępu do systemu Helpdesk, telefonicznie, mailowo, pisemnie lub osobiście	
Inne obowiązki	należy powstrzymać się od wszelkich działań mogących utrudnić ustalenie okoliczności naruszenia, za wyjątkiem działań niezbędnych dla zapewnienia bezpieczeństwa osobom i mieniu	

2.3. **W trakcie realizacji umowy zawartej** ze Szpitalem Uniwersyteckim osoba odpowiedzialna za realizację tej umowy ze strony Szpitala Uniwersyteckiego w porozumieniu z Inspektorem Ochrony Danych **może uznać za konieczne i zażądać podpisania imiennych oświadczeń** o zachowaniu poufności przez Pracowników Dostawcy (Wykonawcy).