Załącznik nr 7
do Regulaminu odbywania w Uniwersyteckim Centrum Klinicznym
staży kierunkowych do specjalizacji przez lekarzy zatrudnionych w innych podmiotach leczniczych

SKIEROWANIE NA SZKOLENIE
Z SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

A	INFORMACJA DLA OSOBY SKIEROWANEJ NA SZKOLENIE

część 1: szkolenie e-learningowe (osoba skierowana na szkolenie zobowiązana jest odbyć szkolenie e-learningowe przed dopuszczeniem do pracy) (szkolenie dostępne jest na stronie głównej UCK – www.uck.pl – w zakładce „Bezpieczeństwo informacji"). Potwierdzenie odbycia tego szkolenia stanowi podpis na dokumencie „Oświadczenie o zachowaniu poufności i zapoznaniu się z przepisami i regulacjami".

część 2: szkolenie stacjonarne z Systemu Zarządzania Bezpieczeństwem Informacji, w tym ochrony danych osobowych, którego dotyczy niniejszy dokument, odbywa się w każdy wtorek lub piątek w budynku nr 9, pok. 318, o godzinie 10:30 (z wyłączeniem dni niepracujących) (osoba skierowana na szkolenie zobowiązana jest odbyć szkolenie najpóźniej w pierwszym tygodniu pracy, czas trwania szkolenia: ok. godziny).

B	SKIEROWANIE NA SZKOLENIE Z SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI
B.1	**Dane osoby kierowanej na przeszkolenie**

……
(imię i nazwisko)
……
(komórka organizacyjna)
……
(stanowisko / świadczona usługa / inne (jakie?)
……
(numer ewidencyjny pracownika)

B.2	Poświadczenie skierowania na przeszkolenie

……
(data, podpis i pieczątka pracownika UCK będące potwierdzeniem skierowania na przeszkolenie)

UCK Uniwersyteckie Centrum Kliniczne

C	ZAŚWIADCZENIE O PRZESZKOLENIU

Zaświadcza się, iż w dniu …… Pan/i ..... zatrudniony/a / świadczący/a usługi / inne (jakie?) ……. w Uniwersyteckim Centrum Klinicznym pod numerem ewidencyjnym …….. odbyła stacjonarne **szkolenie z zakresu Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), w tym szkolenie z zakresu ochrony danych osobowych** obejmujące swoją tematyką omówienie zasad wynikających z:

a) regulacji wewnętrznych UCK, w tym zwłaszcza Polityki Bezpieczeństwa Informacji oraz pozostałej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji,
b) przepisów prawa powszechnie obowiązującego, a zwłaszcza 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 (tzw. ogólnego rozporządzenia o ochronie danych osobowych, RODO).

Szczegółowy program szkolenia:

1. Akty prawne oraz inne regulacje, w tym normy ISO/IEC, z zakresu bezpieczeństwa informacji oraz ochrony danych osobowych.
2. Podstawowe pojęcia i definicje (aktywa informacyjne, informacje, kategorie osób, których dane dotyczą, rodzaje danych, dane osobowe, dane osobowe zwykłe, dane osobowe szczególnej kategorii, dane dotyczące zdrowia, dane genetyczne, dane biometryczne, przetwarzanie danych, zbiór danych, Organ Nadzorczy, Prezes Urzędu Ochrony Danych Osobowych, Administrator, Inspektor Ochrony Danych, Podmiot przetwarzający, Odbiorca danych, Strona trzecia, profilowanie, anonimizacja, pseudonimizacja, obszar przetwarzania informacji, obszar przetwarzania danych osobowych, strefy bezpieczeństwa).
3. Zasady przetwarzania danych osobowych. Zgodność z prawem przetwarzania.
4. Dokumentacja przetwarzania danych osobowych (wymagana dokumentacja i rejestry, upoważnienie do przetwarzania danych osobowych, oświadczenie o zachowaniu poufności).
5. Prawa osoby, której dane dotyczą (prawo do informacji i dostępu do danych, prawo do sprostowania danych, prawo do bycia zapomnianym, prawo do ograniczenia przetwarzania, prawo do przenoszenia danych, prawo do sprzeciwu).
6. Bezpieczeństwo przetwarzania. Zarządzanie ryzykiem. Ocena skutków dla ochrony danych osobowych. *„Privacy by design”*, *„Privacy by default”.*
7. Bezpieczeństwo przetwarzania informacji w praktyce. Podstawowe procedury SZBI, struktura zarządzania bezpieczeństwem informacji w UCK, podstawowe obowiązki pracowników – omówienie powyższego, ze szczególnym uwzględnieniem:
    - zabezpieczeń i wdrożonych polityk, m.in. polityki czystego biurka, polityki czystego ekranu, polityki kluczy i polityki haseł, a także procedur dotyczących rozpoczęcia, zawieszenia i zakończenia pracy w systemach teleinformatycznych UCK,
    - obowiązku poszanowania prawa do prywatności i ochrony informacji różnych kategorii osób, których dane dotyczą (w tym m.in. pacjentów) (organizacja stanowisk, zapewnienie właściwych warunków obsługi).
8. Powierzenie przetwarzania danych osobowych (umowa powierzenia przetwarzania danych osobowych). Umowa o zachowaniu poufności.
9. Incydenty i słabości Systemu Zarządzania Bezpieczeństwem Informacji. Naruszenia ochrony danych osobowych (ODO) (definicje, postępowanie w ramach struktury organizacyjnej UCK, zgłaszanie naruszeń ODO Organowi Nadzorczemu, powiadomienie o naruszeniu ODO osoby, której dane dotyczą).
10. Kontrole PUODO.
11. Odpowiedzialność za naruszenia (dyscyplinarna, karna, odszkodowawcza, administracyjna kara pieniężna)

……

(podpis i pieczątka osoby przeprowadzającej szkolenie)