UNIWERSYTECKI DZIECIĘCY SZPITAL KLINICZNY
im. L. Zamenhofa w Białymstoku

ZASADY REALIZACJI PRAKTYK ZAWODOWYCH STUDENTÓW WNOZ W UNIWERSYTECKIM DZIECIĘCYM SZPITALU KLINICZNYM IM. L. ZAMENHOFA W BIAŁYMSTOKU

I. Dokumenty wymagane do odbycia praktyk zawodowych:

1. Porozumienie/Umowa/Wniosek o praktykę zawodową w dwóch egzemplarzach (osobą wyznaczoną przez Dyrektora do reprezentowania UDSK w Białymstoku jest Elżbieta Sienkiewicz - Z-ca Dyrektora ds. Pielęgniarstwa.
2. Kserokopia polisy OC oraz NNW.
3. Klauzula informacyjna dla studentów odbywających praktyki zawodowe w UDSK w Białymstoku (załącznik nr 1).
4. Podpisane Upoważnienie do przetwarzania danych osobowych w związku z praktykami (załącznik nr 2).
5. Oświadczenie o zapoznaniu się z Instrukcją przetwarzania danych osobowych w Uniwersyteckim Dziecięcym Szpitalu Klinicznym im. L. Zamenhofa w Białymstoku (załącznik nr 3).

II. Procedura uzyskiwania zgody na odbycie praktyk zawodowych

1. Warunkiem odbycia praktyk jest wcześniejsze podpisanie Wniosku na odbycie praktyk.
2. Termin realizacji praktyki należy uzgodnić z Opiekunem praktyk, od którego należy uzyskać akceptację poświadczoną podpisem złożonym na dwóch egzemplarzach Wniosku (termin realizacji praktyki i podpis).
3. Wszystkie wymienione w pkt I, **ułożone w kolejności zgodnej z punktem I.** wypełnione i podpisane dokumenty student powinien złożyć w **Kancelarii Szpitala (I piętro) w wyznaczonych dniach (wtorki i czwartki w godz. 11.00 – 13.00).**
4. Porozumienia/Umowy/Wnioski nie wypełnione, wypełnione nieprawidłowo lub bez w/w załączników nie będą rozpatrywane.
5. W dniu rozpoczęcia praktyki student jest zobowiązany przedstawić opiekunowi praktyki program praktyki oraz polisy OC i NNW.
6. Podpisany Wniosek student odbiera z Kancelarii Szpitala.

UNIWERSYTECKI DZIECIĘCY SZPITAL KLINICZNY
im. L. Zamenhofa w Białymstoku

Załącznik nr 1

Klauzula informacyjna dla studentów odbywających studenckie praktyki zawodowe w UDSK w Białymstoku

W związku z art. 13 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 (RODO), które ma zastosowanie od 25 maja 2018 r., informujemy o przetwarzaniu danych oraz prawach związanych z przetwarzaniem tych danych:

Administrator Danych

Administratorem danych osobowych Pani/Pana jest Uniwersytecki Dziecięcy Szpital Kliniczny im. L. Zamenhofa w Białymstoku.

Dane kontaktowe Inspektora Ochrony Danych

Dane kontaktowe Inspektora Ochrony Danych, z którym można się skontaktować w każdej sprawie dotyczącej przetwarzania danych osobowych, tel. 857450760, e-mail: iodo@udsk.pl

Na jakiej podstawie i w jakim celu przetwarzamy dane?

Pani/Pana dane osobowe będą zbierane i przetwarzane w celu:

a) obsługi praktyk zawodowych na podstawie art. 6 ust. 1 lit. c) RODO; ustawa z dnia 26 czerwca 1974 r. Kodeks Pracy
b) obsługi stażu podyplomowego na podstawie art. 6 ust. 1 lit. c) RODO; ustawa z dnia 26 czerwca 1974 r. Kodeks Pracy; ustawa z dnia 5 grudnia 1996 r. o zawodzie lekarza i lekarza dentysty; Rozporządzenie Ministra z dnia 2 stycznia 2013 r. w sprawie specjalizacji lekarzy i lekarzy dentystów;
c) realizacji celów rachunkowych na podstawie art. 6 ust. 1 lit. c) RODO; ustawa z dnia 29 września 1994 r. o rachunkowości;
d) realizacja celów podatkowych na podstawie art. 6 ust. 1 lit, c) RODO; ustawa z dnia 29 sierpnia 1997 r. Ordynacja podatkowa;
e) archiwizacji dokumentów na podstawie art. 6 ust. 1 lit. c) RODO, ustawa z dnia 20 października 2015 r. w sprawie klasyfikowania i kwalifikowania dokumentacji.

Podanie danych osobowych do powyżej wymienionych celów jest obligatoryjne na mocy przepisów prawa. Niepodanie danych może skutkować uniemożliwieniem Państwu odbycia praktyki zawodowej.

Państwa dane osobowe nie będą przetwarzane w sposób zautomatyzowany, w tym również w formie profilowania, tzn. żadne decyzje wywołujące wobec osoby skutki prawne lub w podobny sposób na nią istotnie wpływające nie będą oparte wyłącznie na automatycznym przetwarzaniu danych osobowych i nie wiążą się z taką automatycznie podejmowaną decyzją.

Komu możemy przekazywać dane?

Dane osobowe mogą być udostępnione uprawnionym podmiotom, na podstawie przepisów prawa. Państwa dane osobowe mogą zostać udostępnione także dostawcom usług i rozwiązań technicznych/organizacyjnych (dostawcy usług IT, firmy kurierskie, pocztowe, ubezpieczyciele, firmy archiwizujące dokumenty, podmioty przeprowadzające szkolenia, itp.), usług prawnych i doradczych (kancelariom prawnym, firmom audytorskim itp.) zgodnie z przepisami w zakresie ochrony danych osobowych oraz pod warunkiem zachowania poufności.

Ile czasu będziemy przechowywać dane?

Państwa dane osobowe przechowywane będą zgodnie z przepisami prawa obowiązującymi w tym zakresie, w szczególności przez czas przewidziany zapisami instrukcji kancelaryjnej. W razie przetwarzania danych osobowych w oparciu o wyrażoną przez Panią/Pana zgodę, Administrator będzie przechowywał Pani/Pana dane do momentu wycofania zgody. Po wskazanym okresie dokumenty zostaną zniszczone.

Prawa związane z przetwarzaniem danych

Mają Państwo prawo do:

a) dostępu do swoich danych oraz otrzymania ich kopii;

b) do sprostowania (poprawiania) swoich danych osobowych;

c) do ograniczenia przetwarzania danych osobowych;

d) do usunięcia danych osobowych;

e) do cofnięcia zgody, gdy przetwarzamy Państwa dane na podstawie udzielonej zgody;

f) prawo do wniesienia skargi do Prezesa UODO (na adres Urzędu Ochrony Danych Osobowych (ul. Stawki 2, 00 - 193 Warszawa).

Informujemy, że Administrator dokłada wszelkich starań, aby zapewnić środki fizycznej, technicznej i organizacyjnej ochrony danych osobowych przed ich przypadkowym czy umyślnym zniszczeniem, przypadkową utratą, zmianą, nieuprawnionym ujawnieniem, wykorzystaniem czy dostępem, zgodnie ze wszystkimi obowiązującymi przepisami.

Zapoznałam/zapoznałem się,

……..

(data i czytelny podpis)

UNIWERSYTECKI DZIECIĘCY SZPITAL KLINICZNY
im. L. Zamenhofa w Białymstoku

Załącznik nr 2

UPOWAŻNIENIE Nr ……./202….

do przetwarzania danych osobowych w związku ze studencką praktyką zawodową

Z dniem **……**na podstawie art. 29 w związku z art. 28 ust. 3 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 osobowych) (Dz. Urz. UE. L 119 z 04.05.2016, str. 1-88), (RODO), upoważniam Pana/Panią*

……

(imię i nazwisko)

do przetwarzania danych osobowych w związku z obywaniem studenckiej praktyki zawodowej

w ……..
(nazwa komórki organizacyjnej, w której będzie realizowana praktyka)

w zakresie wglądu do danych osobowych pacjentów w systemach informatycznych i w dokumentacji tradycyjnej w Uniwersyteckim Dziecięcym Szpitalu Klinicznym im. L. Zamenhofa w Białymstoku.

Upoważnienie wygasa z dniem zakończenia odbywania studenckiej praktyki zawodowej w Uniwersyteckim Dziecięcym Szpitalu Klinicznym im. L. Zamenhofa w Białymstoku.

Jednocześnie informuję, że zobowiązany/-a jest Pan/Pani do zachowania informacji na temat rodzajów oraz sposobów przetwarzania danych w tajemnicy. Obowiązek ten istnieje również po zakończeniu studenckiej praktyki zawodowej.

……..
(data i podpis Administratora Danych)

OŚWIADCZENIE
OSOBY UPOWAŻNIONEJ DO PRZETWARZANIA DANYCH OSOBOWYCH

Ja, niżej podpisany/-a oświadczam, że:
1) przed uzyskaniem dostępu do danych osobowych zapoznałem/-am się z przepisami dotyczącymi ochrony danych osobowych, w szczególności rozporządzeniem 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 2016,119, s.1, Dz. Urz. UE.L 2018,127, s.2 oraz Dz. Urz. UE L 74 z 04.03.2021, str. 35) (w skrócie: RODO) oraz przepisami ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych;
2) znana jest mi treść art. 4 ust. 1 RODO, zgodnie z którym za dane osobowe uważa się wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

3) potwierdzam zapoznanie się z instrukcją w sprawie przetwarzania danych osobowych w UDSK w Białymstoku;
4) zobowiązuję się do przestrzegania przepisów dotyczących ochrony danych osobowych, w tym w szczególności do niewykorzystywania danych w celach niezgodnych z powierzonymi zadaniami, tj. modyfikacji, powielania, usuwania, zapisywania na nośnikach oraz przekazywania danych w dowolnej formie, poza obszar przetwarzania danych i zakres upoważnienia;
5) zobowiązuję się do zachowania w tajemnicy wszelkich informacji związanych z przetwarzanymi danymi oraz o przetwarzaniu danych osobowych, stosowanych środkach zabezpieczeń - technicznych oraz organizacyjnych;
6) mam świadomość ciążącego na mnie obowiązku zachowania w tajemnicy, w okresie odbywania praktyki, jak i po jej zakończeniu danych osobowych, do których uzyskam dostęp;
7) przyjmuję do wiadomości, że niedotrzymanie powyższych zobowiązań będzie stanowiło naruszenie przepisów karnych ustawy o ochronie danych osobowych.

…… .....

(miejscowość, data) *(data i podpis osoby upoważnionej do przetwarzania danych)*

**niepotrzebne skreślić*

UNIWERSYTECKI DZIECIĘCY SZPITAL KLINICZNY
im. L. Zamenhofa w Białymstoku

Załącznik nr 3

Instrukcja przetwarzania danych osobowych

w Uniwersyteckim Dziecięcym Szpitalu Klinicznym im. L. Zamenhofa w Białymstoku

Zgodnie z Polityką ochrony danych osobowych i Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych wymaga się tego, aby:

1. Dostęp do danych osobowych miały wyłącznie osoby posiadające pisemne upoważnienie do przetwarzania danych.
2. Dane były chronione przed dostępem do nich osób nieupoważnionych.
3. Pomieszczenia, w których są przetwarzane dane osobowe, były zamykane na klucz.
4. Dostęp do kluczy posiadali tylko upoważnieni pracownicy.
5. Dostęp do pomieszczeń był możliwy tylko i wyłącznie w godzinach pracy. W sytuacji gdy jest wymagany poza godzinami pracy – tylko na podstawie zezwolenia administratora danych.
6. Dostęp do pomieszczeń, w których są przetwarzane dane osobowe, mogli mieć tylko osoby upoważnione.
7. W przypadku pomieszczeń, do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych i tylko w czasie wymaganym na wykonanie niezbędnych czynności.
8. Szafy, w których przechowywane są dane, były zamykane na klucz.
9. Klucze do tych szaf posiadali tylko upoważnione osoby.
10. Szafy z danymi były otwarte tylko na czas potrzebny na dostęp do danych, a następnie były zamykane.
11. Dane w formie papierowej znajdowały się na biurkach tylko na czas niezbędny do wykonania czynności służbowych, a następnie były chowane do szaf.
12. Dostęp do komputerów, na których są przetwarzane dane, mieli tylko upoważnieni pracownicy/stażyści.
13. Monitory komputerów, na których są przetwarzane dane, były tak ustawione, aby osoby nieupoważnione nie miały wglądu w dane.
14. Przed choćby chwilowym opuszczeniem miejsca pracy, należy blokować stację roboczą komputera stosując skrót klawiszowy: „WINDOWS + L„
15. W razie potrzeby wyniesienia komputera przenośnego (np. typu notebook), zawierającego dane osobowe lub inne informacje chronione, komputer taki był odpowiednio dodatkowo zabezpieczony, a dane zaszyfrowane. Fakt taki niezwłocznie zgłaszany jest informatykom.

16. Nie udostępniać osobom nieupoważnionym tych komputerów.

17. Nie korzystać w trakcie pracy z prywatnej poczty elektronicznej. Nie otwierać podejrzanych maili z niewiadomego pochodzenia.

18.Nie podłączać zewnętrznych nośników danych do komputerów, np. pendrivów.

19. Użytkownicy przynajmniej raz w miesiącu dokonywali przeglądu skrzynek mailowych i usuwali z nich stare i nieprzydatne wiadomości.

20. Stosować procedurę szyfrowania danych. W przypadku zaistnienia konieczności przesłania drogą elektroniczną dokumentu z danymi, załącznik powinien zostać uprzednio zaszyfrowany, zaś hasło do pliku przesłane drugim nośnikiem.

21. Sieć komputerowa była zabezpieczona przed wszelkim dostępem z zewnątrz.

22. Błędne lub nieaktualne wydruki i wersje papierowe zawierające dane osobowe lub inne informacje chronione były niszczone za pomocą niszczarki lub w inny mechaniczny sposób uniemożliwiający powtórne ich odtworzenie.

23. Nie instalować samodzielne jakichkolwiek programów w systemach informatycznych bez zgody i wiedzy Dyrekcji i Informatyków.

24. Dbać o aktualizacje systemów operacyjnych oraz oprogramowani antywirusowych (fakt ten, należy zgłosić do Działu IT).

25. Wszelkie problemy, usterki i incydenty w systemach informatycznych zgłaszane były do Działu IT.

26. Wszelkie naruszenia danych osobowych zgłaszane były pod rygorem odpowiedzialności pracowniczej administratorowi danych – Dyrekcji.

Za prawidłowy nadzór przetwarzania danych oraz zapewnienie im odpowiedniej ochrony odpowiada każdy pracownik/stażysta na swoim stanowisku pracy, zgodnie z zakresem obowiązków.

Za nieprzestrzeganie procedur bezpieczeństwa i naruszenie ochrony danych grozi odpowiedzialność finansowa, odszkodowawcza, dyscyplinarna, a w skrajnych przypadkach nawet karna.

Przypadki zakwalifikowane jako **naruszenie (incydent)** lub uzasadnione podejrzenie naruszenia zabezpieczenia danych osobowych to głównie:

1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, kradzież, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.;

2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy;

3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku

naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru;

4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;

5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie;

6) naruszenie lub próba naruszenia integralności systemu albo bazy danych;

7) próbę modyfikacji lub modyfikacja danych albo zmiana w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);

8) niedopuszczalna manipulacja danymi osobowymi w systemie;

9) ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedury ochrony przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń;

10) praca w systemie lub jego sieci komputerowej wykazująca nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony informacji – np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.;

11) istnienie nieautoryzowanych kont dostępu do danych lub tzw. bocznej furtki, itp.;

12) podmiana lub zniszczenie nośników z danymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowanie bądź skopiowanie danych;

13) rażące naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych, zgubienie nośników z danymi, itp.). Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych, tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.

Przeczytałem poniższy instruktaż, w pełni go zrozumiałem/-am i zaakceptowałem/-am. Zobowiązuję się go przestrzegać, co potwierdzam własnoręcznym podpisem.

……

(data i podpis osoby upoważnionej do przetwarzania danych)