ZAŁĄCZNIK DO UMOWY

POROZUMIENIE W SPRAWIE UDOSTĘPNIANIA I ZABEZPIECZENIA DANYCH OSOBOWYCH

POMIĘDZY ODRĘBNYMI ADMINISTRATORAMI

w związku z realizacją świadczeń teleradiologicznej diagnostyki obrazowej
znak sprawy: 2/PDO/OB/2026

zawarte w dniu ..... r. pomiędzy:

Zespołem Opieki Zdrowotnej w Nidzicy, ul. Mickiewicza 23, 13-100 Nidzica, KRS 0000000627, REGON 00030656100000, NIP 9840078782, reprezentowanym przez Dyrektora - Pawła Szulca, zwanym dalej "Udzielającym Zamówienia",

a

.....,

reprezentowanym przez .....,

zwanym dalej "Przyjmującym Zamówienie",

łącznie zwanymi dalej "Stronami".

Porozumienie określa zasady udostępniania i zabezpieczenia danych osobowych w związku z realizacją umowy o udzielanie świadczeń zdrowotnych w zakresie teleradiologii, zwanej dalej "Umową główną".

§ 1. Status Stron

1. Każda ze Stron jest odrębnym administratorem danych osobowych przetwarzanych w związku z realizacją Umowy głównej, w zakresie celów i sposobów przetwarzania określanych samodzielnie przez daną Stronę na podstawie obowiązujących przepisów prawa.
2. Przyjmujący Zamówienie samodzielnie udziela świadczeń zdrowotnych w zakresie teleradiologii, w szczególności dokonuje oceny badań obrazowych, sporządza i autoryzuje opisy, przekazuje wyniki oraz prowadzi dokumentację medyczną w zakresie wymaganym przepisami prawa.
3. Udostępnianie danych w celu udzielania świadczeń zdrowotnych nie stanowi powierzenia przetwarzania danych osobowych w rozumieniu art. 28 RODO ani ustanowienia współadministratorów w rozumieniu art. 26 RODO.
4. Każda ze Stron samodzielnie odpowiada za zgodność z prawem wykonywanych przez siebie operacji przetwarzania, realizację praw osób, obowiązków informacyjnych oraz obowiązków dotyczących bezpieczeństwa danych.

§ 2. Cel i podstawy udostępniania danych

1. Dane są udostępniane w zakresie niezbędnym do wykonania Umowy głównej, w szczególności w celu wykonania opisów badań MR, TK i RTG, zapewnienia ciągłości świadczeń zdrowotnych, prowadzenia dokumentacji medycznej, obsługi korekt, konsultacji i wyników krytycznych oraz rozliczenia i kontroli świadczeń.
2. Podstawę przetwarzania stanowią w szczególności art. 6 ust. 1 lit. c oraz art. 9 ust. 2 lit. h RODO, art. 26 ust. 3 pkt 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta oraz właściwe przepisy dotyczące działalności leczniczej, dokumentacji medycznej i teleradiologii.
3. Dane nie mogą być wykorzystywane do celów marketingowych, tworzenia baz danych niezwiązanych z realizacją świadczeń, profilowania komercyjnego ani trenowania lub rozwijania modeli lub systemów sztucznej inteligencji, chyba że odrębna podstawa prawna i warunki takiego przetwarzania zostały uprzednio wykazane i uzgodnione zgodnie z prawem.

§ 3. Kategorie osób i zakres danych

1. Udostępnienie dotyczy pacjentów, których badania przekazywane są do opisu, oraz - w niezbędnym zakresie - lekarzy, personelu medycznego i osób uczestniczących w obsłudze Umowy głównej.
2. Udzielający Zamówienia udostępnia w szczególności:
   1) dane identyfikacyjne pacjenta, w tym imię i nazwisko, numer PESEL lub inny identyfikator, datę urodzenia i płeć;
   2) dane zawarte w skierowaniu lub zleceniu, informacje kliniczne oraz dane dotyczące stanu zdrowia niezbędne do wykonania opisu;
   3) obrazy diagnostyczne MR, TK i RTG wraz z metadanymi DICOM;
   4) wcześniejsze wyniki badań lub inną dokumentację niezbędną do prawidłowej oceny i zachowania ciągłości świadczeń;
   5) dane lekarza kierującego, zlecającego oraz personelu uczestniczącego w realizacji badania.
3. Przyjmujący Zamówienie przekazuje w szczególności autoryzowany opis badania, dane lekarza opisującego, informacje o wyniku krytycznym, zalecenia wynikające z opisu oraz informacje o odmowie wykonania opisu wraz z jej przyczyną.

4. Strony stosują zasadę minimalizacji danych i udostępniają wyłącznie dane adekwatne i niezbędne do realizacji określonego celu.

§ 4. Poufność i personel

1. Każda ze Stron zapewnia, że dostęp do danych mają wyłącznie osoby, dla których jest to niezbędne do wykonywania obowiązków związanych z realizacją Umowy głównej.
2. Osoby mające dostęp do danych posiadają odpowiednie upoważnienia oraz są zobowiązane do zachowania poufności, tajemnicy medycznej i zasad bezpieczeństwa informacji także po ustaniu współpracy.
3. Każda ze Stron odpowiada za nadawanie, zmianę, okresowy przegląd i odbieranie uprawnień w systemach pozostających pod jej kontrolą.

§ 5. Środki techniczne i organizacyjne

1. Każda ze Stron wdraża i utrzymuje środki techniczne i organizacyjne odpowiednie do ryzyka, z uwzględnieniem szczególnego charakteru danych dotyczących zdrowia oraz konieczności zapewnienia ciągłości świadczeń.
2. Środki obejmują, odpowiednio do stosowanych rozwiązań:
   1) szyfrowanie transmisji i stosowanie bezpiecznych połączeń, w tym VPN, jeżeli jest wykorzystywany;
   2) indywidualne konta, silne uwierzytelnianie, kontrolę uprawnień oraz uwierzytelnianie wieloskładnikowe dla dostępu zdalnego lub uprzywilejowanego;
   3) rejestrowanie istotnych operacji i zdarzeń oraz ochronę logów;
   4) zabezpieczenie stacji roboczych, serwerów i sieci, aktualizacje bezpieczeństwa oraz ochronę przed złośliwym oprogramowaniem;
   5) kopie zapasowe, procedury odtworzeniowe i rozwiązania zapewniające ciągłość działania;
   6) regularne testowanie i ocenę skuteczności zabezpieczeń;
   7) fizyczne zabezpieczenie miejsc i urządzeń, w których dane są przetwarzane.
3. Na uzasadnione żądanie druga Strona przedstawia opis stosowanych zabezpieczeń w zakresie pozwalającym ocenić ich adekwatność, bez ujawniania informacji, których ujawnienie mogłoby obniżyć poziom bezpieczeństwa lub naruszyć prawa innych podmiotów.

§ 6. Systemy, transmisja i ciągłość

1. Przekazywanie obrazów, opisów i innych danych odbywa się przy użyciu zabezpieczonych systemów teleinformatycznych i kanałów komunikacji uzgodnionych przez Strony.
2. Każda ze Stron odpowiada za zabezpieczenie systemów, urządzeń i infrastruktury pozostających pod jej kontrolą.
3. Środki ochrony danych nie mogą powodować nieuzasadnionego ograniczenia dostępu do danych i opisów niezbędnych do udzielania świadczeń, w szczególności w trybie CITO i CITO-CITO.
4. Awarie i incydenty wpływające na dostępność lub bezpieczeństwo danych podlegają procedurom określonym w Umowie głównej oraz niniejszym Porozumieniu.

§ 7. Naruszenia ochrony danych

1. Strona, która stwierdzi naruszenie ochrony danych mogące dotyczyć danych udostępnianych w związku z Umową główną, informuje drugą Stronę bez zbędnej zwłoki, nie później niż w ciągu 24 godzin od stwierdzenia naruszenia.
2. Zawiadomienie przekazuje się na adres iod@zoz.nidzica.pl oraz na dane kontaktowe wskazane przez Przyjmującego Zamówienie i, w zakresie dostępnym na danym etapie, obejmuje ono opis zdarzenia, kategorie danych i osób, przybliżoną liczbę osób i rekordów, możliwe konsekwencje, zastosowane lub planowane środki zaradcze, czas wykrycia i dane osoby kontaktowej.
3. Każda ze Stron samodzielnie ocenia i realizuje obowiązek zgłoszenia naruszenia Prezesowi Urzędu Ochrony Danych Osobowych oraz zawiadomienia osób, których dane dotyczą, w zakresie przetwarzania, za które odpowiada.
4. Strony współpracują przy ustalaniu okoliczności, przyczyn i skutków naruszenia oraz zabezpieczeniu dowodów i ograniczeniu ryzyka, z poszanowaniem niezależności każdego administratora.

§ 8. Podmioty wspierające Strony

1. Każda ze Stron może korzystać z podmiotów przetwarzających dane w jej imieniu, pod warunkiem samodzielnego zapewnienia zgodności takiej relacji z art. 28 RODO.
2. Strona korzystająca z podmiotu przetwarzającego odpowiada za zawarcie wymaganej umowy, dobór podmiotu zapewniającego wystarczające gwarancje oraz nadzór nad wykonywanym przetwarzaniem.
3. Przyjmujący Zamówienie, przed rozpoczęciem realizacji świadczeń, przekazuje Udzielającemu Zamówienia informację o lokalizacji systemów i serwerów wykorzystywanych do realizacji Umowy głównej oraz o podmiotach zapewniających hosting, transmisję, utrzymanie lub inne usługi techniczne związane z dostępem do danych.

4. Jeżeli w ramach współpracy jedna ze Stron miałaby wykonywać na rzecz drugiej odrębne czynności techniczne wyłącznie na jej udokumentowane polecenie i w jej imieniu, Strony przed rozpoczęciem takich czynności zawrą odrębną umowę zgodną z art. 28 RODO, ograniczoną do tego zakresu. Umowa ta nie obejmuje samodzielnego udzielania i dokumentowania świadczeń zdrowotnych.

§ 9. Miejsce przetwarzania i transfery poza EOG

1. Dane związane z realizacją Umowy głównej są przetwarzane na terytorium Europejskiego Obszaru Gospodarczego, chyba że właściwy administrator zapewni zgodny z prawem mechanizm transferu oraz uprzednio poinformuje drugą Stronę o planowanym przekazaniu lub dostępie z państwa trzeciego.
2. Na uzasadnione żądanie Strona wskazuje lokalizacje centrów danych, kopii zapasowych oraz miejsca, z których możliwy jest administracyjny lub medyczny dostęp do danych związanych z realizacją Umowy głównej.

§ 10. Prawa osób i obowiązki informacyjne

1. Każda ze Stron realizuje obowiązki informacyjne i żądania osób, których dane dotyczą, w zakresie przetwarzania prowadzonego przez siebie jako odrębnego administratora.
2. Jeżeli Strona otrzyma żądanie dotyczące przetwarzania prowadzonego przez drugą Stronę, przekazuje je właściwej Stronie bez zbędnej zwłoki, o ile jest możliwe ustalenie właściwości i przekazanie jest zgodne z prawem.
3. Strony udzielają sobie niezbędnej pomocy informacyjnej, nie przejmując odpowiedzialności drugiego administratora.

§ 11. Przechowywanie danych i dokumentacji

1. Każda ze Stron przechowuje dokumentację medyczną i inne dane przez okres wynikający z przepisów prawa oraz własnych obowiązków jako administratora.
2. Zakończenie Umowy głównej nie powoduje obowiązku usunięcia danych lub dokumentacji, które dana Strona ma obowiązek albo uprawnienie przechowywać na podstawie prawa.
3. Dane, dla których nie istnieje dalsza podstawa przetwarzania, podlegają usunięciu lub anonimizacji zgodnie z procedurami właściwego administratora, z uwzględnieniem cyklu nadpisywania kopii zapasowych.

§ 12. Weryfikacja bezpieczeństwa

1. Na uzasadnione żądanie Strony udostępniają sobie informacje niezbędne do potwierdzenia spełnienia wymagań bezpieczeństwa określonych w Umowie głównej i niniejszym Porozumieniu.
2. Udzielający Zamówienia może zweryfikować zabezpieczenia dotyczące transmisji, integracji i realizacji świadczeń, po uprzednim uzgodnieniu terminu i zakresu, z wyjątkiem sytuacji wymagających niezwłocznego działania z powodu incydentu lub żądania uprawnionego organu.
3. Weryfikacja nie może naruszać tajemnicy przedsiębiorstwa, bezpieczeństwa systemów, dokumentacji innych pacjentów ani praw innych administratorów i ich klientów.

§ 13. Odpowiedzialność

1. Każda ze Stron ponosi odpowiedzialność za naruszenia przepisów o ochronie danych, praw pacjenta, tajemnicy medycznej oraz postanowień niniejszego Porozumienia wynikające z jej działań lub zaniechań.
2. Każda ze Stron odpowiada za osoby działające z jej upoważnienia oraz za podmioty przetwarzające, z których korzysta.
3. Odpowiedzialność Stron określają RODO, przepisy prawa krajowego i Umowa główna.

§ 14. Postanowienia końcowe

1. Porozumienie obowiązuje od dnia rozpoczęcia udostępniania danych, nie wcześniej niż od dnia wejścia w życie Umowy głównej, i przez okres niezbędny do wykonania obowiązków Stron związanych z przetwarzaniem danych.
2. W razie sprzeczności pomiędzy niniejszym Porozumieniem a Umową główną w zakresie statusu Stron i zasad udostępniania danych pierwszeństwo mają postanowienia niniejszego Porozumienia, z zastrzeżeniem przepisów bezwzględnie obowiązujących.
3. Zmiana Porozumienia wymaga formy właściwej dla Umowy głównej, z wyjątkiem aktualizacji danych kontaktowych, które mogą być dokonywane w formie dokumentowej.
4. W sprawach nieuregulowanych stosuje się RODO, ustawę o prawach pacjenta i Rzeczniku Praw Pacjenta oraz pozostałe właściwe przepisy prawa polskiego i prawa Unii Europejskiej.

UDZIELAJĄCY ZAMÓWIENIA	**PRZYJMUJĄCY ZAMÓWIENIE**
.....	.....