UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Umowa powierzenia przetwarzania danych osobowych Nr ……
*(zwana dalej „**Umową**”)*

zawarta w dniu …… w Suchej Beskidzkiej pomiędzy:

Zespołem Opieki Zdrowotnej w Suchej Beskidzkiej z siedzibą w Suchej Beskidzkiej, ul. Szpitalna 22;
REGON 000304415,
którego reprezentuje:
Dyrektor – lek. Marek Haber
zwanym dalej „**Administratorem**”,
a
Firmą: ……
z siedzibą: ……
NIP: ……, Regon: ……
którą reprezentuje: ……
zwaną dalej **„Podmiotem przetwarzającym”,**
o następującej treści:

§ 1

1. **Strony** łączy umowa Nr …….. zawarta w dniu …… w przedmiocie: **opisywanie badań tomografii komputerowej**
2. **Administrator** danych oświadcza, że powierzane dane osobowe zostały zgromadzone zgodnie z obowiązującymi przepisami prawa i jest uprawniony do ich powierzania.
3. **Podmiot przetwarzający** oświadcza, że dysponuje środkami technicznymi i organizacyjnymi umożliwiającymi prawidłowe przetwarzanie danych osobowych powierzonych przez **Administratora**, w zakresie i celu określonym umową.

§ 2

1. Na podstawie 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) zwanego dalej „RODO”, **Administrator** danych powierza **Podmiotowi przetwarzającemu** przetwarzanie danych osobowych wyłącznie w celu realizacji przedmiotu umowy Nr …… z dnia ……. (zwanej dalej umową podstawową).
2. Dostęp do danych odbywa się poprzez szyfrowane łącze VPN zestawione przez **Administratora**.
3. Przetwarzane dane, to wrażliwe dane medyczne, dotyczące stanu zdrowia pacjentów.
4. Zakres powierzonych danych jest następujący:

1) informacje obejmujące dane pacjentów:
   a) nazwisko i imię (imiona);
   b) data urodzenia;
   c) oznaczenie płci;
   d) adres miejsca zamieszkania/oddział szpitalny;
   e) numer PESEL, jeżeli został nadany, w przypadku noworodka – numer PESEL matki, a w przypadku osób, które nie mają nadanego numeru PESEL – rodzaj i numer dokumentu potwierdzającego tożsamość;
   f) w przypadku gdy pacjentem jest osoba małoletnia, całkowicie ubezwłasnowolniona lub niezdolna do świadomego wyrażenia zgody – nazwisko i imię (imiona) przedstawiciela ustawowego oraz adres jego miejsca zamieszkania;

g) numer identyfikacyjny pacjenta podawany przy braku innych danych;
h) rozpoznanie ustalone przez osobę kierującą;
i) inne informacje lub dane, w zakresie niezbędnym do przeprowadzenia badania, konsultacji lub leczenia.

2) informacje w zakresie danych personelu **Administratora**

Zakres danych osobowych, określonych w § 2 ust. 4 ppt 1, jest maksymalnym katalogiem danych, które mogą być przetwarzane w związku z realizacją Umowy podstawowej. W rzeczywistości dane mogą być przekazywane przez **Administratora** w mniejszym zakresie bez uszczerbku dla postanowień Umowy. Zakres danych może ulec zmianie w przypadku zmiany aktualnie obowiązujących przepisów prawa oraz ustaleń umownych między **Stronami**.

5. **Podmiot przetwarzający** zobowiązuje się do przetwarzania powierzonych danych osobowych wyłącznie w celach związanych z realizacją umowy podstawowej, wyłącznie w miejscu i zakresie jaki jest niezbędny do realizacji tych celów.

6. **Podmiot przetwarzający** jest zobowiązany do zabezpieczenia powierzonego mu certyfikatu i hasła służącego do zestawienia połączenia VPN przed dostępem jakichkolwiek innych osób.

7. Nadany przez **Administratora** certyfikat i hasło służące do zestawienia połączenia VPN są ważne przez okres 1 roku od ich nadania.

8. Niniejsza umowa zostaje zawarta na czas obowiązywania umowy podstawowej. Po zakończeniu obowiązywania umowy podstawowej Podmiot przetwarzający zobowiązany jest do natychmiastowego zwrotu znajdujących się w jego posiadaniu, a przekazanych przez Administratora danych osobowych.

§ 3

1. **Strony** zobowiązują się wykonywać zobowiązania wynikające z niniejszej umowy z najwyższą starannością zawodową w celu zabezpieczenia prawnego, organizacyjnego i technicznego interesów **Stron** w zakresie przetwarzania powierzonych danych osobowych.

2. **Strony** są zobowiązane do wzajemnego niezwłocznego powiadamiania drugiej **Strony**, o każdej kontroli uprawnionych organów w obszarze powierzonych danych, w tym również po zakończeniu okresu związania **Stron** umową podstawową.

3. **Strony** są zobowiązane solidarnie współdziałać w zakresie wywiązywania się z obowiązków odpowiadania na żądania osób, których dane dotyczą.

4. **Podmiot przetwarzający** zobowiązuje się zastosować środki techniczne i organizacyjne mające na celu należyte, odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, zabezpieczenie powierzonych do przetwarzania danych osobowych, w szczególności zabezpieczyć je przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa, oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, zgodnie z art. 32 RODO.

5. **Podmiot przetwarzający** przetwarza dane osobowe wyłącznie na udokumentowane polecenie **Administratora**, chyba że obowiązek taki nakładają na niego przepisy powszechnie obowiązującego prawa.

6. **Podmiot przetwarzający** oświadcza, że posiada upoważnienie nadane przez **Administratora** upoważniające do przetwarzanych danych osobowych w odpowiednim zakresie i został przeszkolony z zakresu bezpieczeństwa informacji, jak również, że został zobowiązany do zachowania w tajemnicy wszelkich danych, w tym odnoszących się do sposobu ich zabezpieczenia.

7. **Podmiot przetwarzający** oświadcza, że zastosowane do przetwarzania powierzonych danych systemy informatyczne oraz sprzęt komputerowy spełniają wymogi aktualnie obowiązujących przepisów prawa, w tym przepisów RODO.

8. **Podmiot przetwarzający** po zakończeniu świadczenia usług związanych z przetwarzaniem skutecznie usuwa wszelkie dane osobowe oraz istniejące kopie chyba, że szczególne przepisy prawa nakazują przechowywanie danych osobowych.

9. **Podmiot przetwarzający** udostępnia **Administratorowi** wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszej umowie oraz umożliwia

Administratorowi lub audytorowi upoważnionemu przez **Administratora** przeprowadzanie audytów i kontroli.

10. **Podmiot przetwarzający** nie korzysta z usług innego **Podmiotu przetwarzającego**.

11. **Podmiot przetwarzający** jest obowiązany do niezwłocznego, nie dłuższego niż 24 godziny, powiadomienia **Administratora** o wszelkich przypadkach naruszenia ochrony powierzonych danych osobowych.

12. W sytuacji naruszenia ochrony powierzonych danych osobowych przez **Podmiot przetwarzający** lub podejrzewania takiego naruszenia**, Administrator** dokona wyłączenia łącza VPN.

13. Na wniosek **Administratora Podmiot przetwarzający** jest zobowiązany do udzielenia informacji na temat przetwarzania powierzonych danych osobowych, w tym na temat zastosowanych przy przetwarzaniu danych osobowych środków technicznych i organizacyjnych, w terminie do 14 dni od otrzymania wniosku.

14. **Administrator** może przeprowadzić audyt u przetwarzającego by ocenić stopień spełnienie wymagań bezpieczeństwa wymaganych przez RODO, lecz nie częściej niż raz na 6 miesięcy.

15. Audyt, o którym mowa w ust. 13, nie musi być przeprowadzany jeżeli **Podmiot przetwarzający** przedstawi ważny certyfikat, o którym mowa w art. 42 RODO.

§ 4

1. Ponoszenie przez **Administratora** odpowiedzialności za przestrzeganie przepisów prawa w zakresie przetwarzania i ochrony danych osobowych według rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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) nie wyłącza odpowiedzialności **Podmiotu przetwarzającego** wyłącznie za przetwarzanie danych niezgodnie z przepisami ww. ogólnego rozporządzenia o ochronie danych, które nakładają obowiązki bezpośrednio na podmioty przetwarzające lub gdy działał on poza zgodnymi z prawem pisemnymi instrukcjami Administratora lub wbrew tym instrukcjom

2. **Podmiot przetwarzający** odpowiada w pełnej wysokości za szkody spowodowane przetwarzaniem, jeśli nie dopełnił obowiązków, które przepisy ww. ogólnego rozporządzenia o ochronie danych nakładają bezpośrednio na podmioty przetwarzające lub gdy działał poza zgodnymi z prawem pisemnymi instrukcjami **Administratora** lub wbrew tym instrukcjom.

§ 5

1. Wszelkie zmiany niniejszej umowy powinny być dokonane w formie pisemnej pod rygorem nieważności.

2. W przypadku, gdy niniejsza umowa odwołuje się do przepisów prawa, oznacza to również inne przepisy dotyczące ochrony danych osobowych, a także wszelkie nowelizacje, jakie wejdą w życie po dniu zawarcia umowy, jak również akty prawne, które zastąpią wskazane ustawy i rozporządzenia.

3. **Strony** postanawiają, że osobą odpowiedzialną za realizację postanowień niniejszej umowy jest:

a) ze **Strony Podmiotu przetwarzającego** - ……..……, e-mail: ……..…….

b) ze **Strony Administratora** - Marek Sadowski, e-mail: **masad@zozsuchabeskidzka.pl**

4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze **Stron**.

5. Wszelkie spory wynikłe z niniejszej umowy rozstrzygane będą przez sąd właściwy miejscowo dla siedziby **Administratora**.

6. Niniejsza umowa powierzenia przetwarzania danych obowiązuje na czas trwania umowy podstawowej począwszy od dnia …….. r.

……..	……
Podmiot przetwarzający	**Administrator**