Załącznik nr 4 do umowy z dnia ………………………………….

**(projekt) Umowa powierzenia przetwarzania danych osobowych**

zawarta w Łodzi w dniu ………………………….. pomiędzy:

**Miejskim Centrum Medycznym „Bałuty” w Łodzi** ul. Bydgoska 17/21 działającym zgodnie z wpisem do Krajowego Rejestru Sądowego w Sądzie Rejonowym dla Łodzi – Śródmieścia w Łodzi pod numerem KRS 0000018267,

NIP: 726-22-51-379, REGON: 000313319

zwanym w dalszej treści umowy **„Administratorem danych” lub „Administratorem”**

reprezentowanym przez:

 Dyrektora - ……………………………………….

a

……………………………………………………………………………………………..

……………………………………………………………………………………………..

reprezentowaną przez: ........................................................

zwany w dalszej części umowy **„Podmiotem przetwarzającym”**

**§ 1**

**Powierzenie przetwarzania danych osobowych**

1. Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 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 w dalszej części „Rozporządzeniem” dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.

**§2**

**Zakres i cel przetwarzania danych**

1. Podmiot przetwarzający może przetwarzać dane osobowe przekazane przez Administratora wyłącznie w celu wykonania umowy podstawowej zawartej w dniu …………………….. r., której przedmiotem jest wykonywanie badań laboratoryjnych, w zakresie niezbędnym do wykonania ww. umowy w zakresie zbierania, utrwalania, przeglądania, pobierania, wykorzystania, udostępniania, przechowywania, adaptowania lub modyfikowania, usuwania lub niszczenia.
2. Administrator powierza Podmiotowi przetwarzającemu dane charakteryzujące osobę, której udzielono świadczenie zdrowotne, oraz dane związanych z udzielonym świadczeniem w zakresie następujących kategorii danych:
* pacjent – imię ( imiona) i nazwisko, numer PESEL, adres zamieszkania, płeć, nr telefonu,

dane zdrowotne, materiał biologiczny. W przypadku osób, który które nie mają nadanego nr PESEL data urodzenia, rodzaj i numer dowodu potwierdzającego tożsamość i w przypadku noworodka numer PESEL matki, imię i nazwisko przedstawiciela ustawowego oraz adres jego miejsca zamieszkania.

* osoby zlecającej świadczenie – imię nazwisko, stanowisko, nr prawa wykonywania zawodu.
1. Zmiana zakresu oraz celu przetwarzania danych osobowych może zostać dokonana jedynie w drodze zmiany niniejszej Umowy.

**§ 3**

**Obowiązki podmiotu przetwarzającego**

Podmiot przetwarzający zobowiązany jest do:

1. podjęcia przed rozpoczęciem dokonywania przetwarzania danych osobowych na podstawie Umowy i stosowania przez cały czas trwania przetwarzania danych osobowych środków organizacyjnych i technicznych zapewniających odpowiedni stopień bezpieczeństwa danych osobowych w tym m.in.:
2. zapewnieniu przez cały czas poufności, integralności, dostępności i odporności systemów oraz usług przetwarzania;
3. przywróceniu dostępności oraz dostępu do powierzonych danych osobowych w sposób terminowy w przypadku awarii fizycznej lub technicznej;
4. regularnym testowaniu, ocenie i ewaluacji efektywności środków technicznych i organizacyjnych dla bezpieczeństwa przetwarzania danych osobowych;
5. wdrożeniu i utrzymaniu kontroli bezpieczeństwa oraz zabezpieczeń w celu spełnienia wymogów właściwych przepisów w zakresie ochrony danych.
6. prowadzenia wymaganej obowiązującymi przepisami o ochronie danych osobowych dokumentacji ochrony danych;
7. współpracy, na każde żądanie, z jakimkolwiek organem nadzorczym uprawnionym do kontroli przestrzegania przepisów o ochronie danych w zakresie i sposób określonych przez ten organ;
8. dokumentowania wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutków oraz podjętych działaniach zaradczych;
9. regularnej weryfikacji i aktualizacji stosowanych przez niego środków technicznych i organizacyjnych tak, aby zapewnić powierzonym danym osobowym adekwatny stopień ochrony. Podmiot przetwarzający, na każde żądanie Administratora danych, przekaże informacje o stosowanych przez niego środkach organizacyjnych i technicznych związanych z przetwarzaniem danych osobowych.
10. dołożenia należytej staranności przy przetwarzaniu powierzonych danych osobowych.
11. współpracowania i udzielania wszelkiej pomocy Administratorowi w celu wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia. W szczególności Podmiot przetwarzający będzie udzielał Administratorowi wszelkich informacji dotyczących stosowanych środków bezpieczeństwa, certyfikacji w określonych obszarach, zidentyfikowanych po stronie Podmiotu przetwarzającego ryzyk związanych z przetwarzaniem danych osobowych oraz wspierał Administratora przy przeprowadzaniu analizy ryzyka lub oceny skutków dla ochrony danych poprzez udzielanie Administratorowi niezbędnych informacji odnośnie przetwarzania danych osobowych przez Podmiot przetwarzający potrzebnych do przeprowadzenia przez Administratora analizy ryzyka lub oceny skutków dla ochrony danych zapewnienia by:
12. dostęp do danych osobowych miały wyłącznie osoby upoważnione do tego przez Podmiot przetwarzający;
13. osoby upoważnione do przetwarzania danych osobowych zobowiązały się na piśmie do zachowania w tajemnicy tych danych osobowych oraz do przestrzegania sposobów ich zabezpieczenia.

**§ 4**

1. Podmiot przetwarzający zobowiązany jest do niezwłocznego poinformowania Administratora *za pośrednictwem poczty elektronicznej na adres: dpo@mcmbaluty.pl* o:
2. jakimkolwiek postępowaniu lub orzeczeniu dotyczącym danych osobowych, w tym zwłaszcza ich prawidłowego zabezpieczenia;
3. stwierdzonym przez Podmiot przetwarzający naruszeniu ochrony danych osobowych, w tym w szczególności danych osobowych lub zagrożeniu takiego naruszenia nie później niż w ciągu 24 godzin od wykrycia naruszenia, wraz ze wskazaniem (opisem):
* charakteru naruszenia ochrony danych osobowych, w tym kategorii i przybliżonej liczby osób, których dane dotyczą;
* możliwych konsekwencji naruszenia ochrony danych osobowych;
* środków zastosowanych lub proponowanych przez Podmiot przetwarzający w celu zaradzenia naruszeniu ochrony danych osobowych, w tym środków mających na celu zminimalizowanie jego ewentualnych negatywnych skutków;
* dane kontaktowe inspektora ochrony danych,
1. zapowiedzi albo rozpoczęciu przez organ nadzorczy kontroli lub postępowania wyjaśniającego dotyczącego danych osobowych;
2. podmiot przetwarzający po zakończeniu świadczenia usług związanych
z przetwarzaniem usuwa wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, w czasie przewidzianym przez aktualnie obowiązujące prawo w zakresie przechowywania danych medycznych na swój koszt.

**§ 5**

**Prawo audytu**

1. Administrator danych zgodnie z art. 28 ust. 3 pkt h) uprawniony jest do przeprowadzania audytu Podmiotu przetwarzającego w zakresie zgodności wykonywania przez niego czynności przetwarzania danych osobowych z postanowieniami Umowy oraz obowiązującymi przepisami o ochronie danych, w szczególności w celu sprawdzenia wykonywania przez Podmiot przetwarzający ciążących na nim obowiązków.
2. Administrator danych realizować będzie prawo audytu w godzinach pracy Podmiotu przetwarzającego O zamiarze przeprowadzenia audytu Administrator zobowiązany jest zawiadomić Podmiot przetwarzający z co najmniej 7 dniowym wyprzedzeniem, przy czym w przypadku uzyskania przez Administratora informacji o rażącym naruszeniu przez Podmiot przetwarzający obowiązków wynikających z Rozporządzenia, przepisów o ochronie danych osobowych lub Umowy, Administrator uprawniony jest do przeprowadzenia audytu bez uprzedniego zawiadomienia.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas audytu w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni .
4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

**§ 6**

**Dalsze powierzenie danych do przetwarzania**

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora danych.
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora danych.
3. Podwykonawca, o którym mowa w § 6 ust. 1 Umowy winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający
w niniejszej Umowie.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

**§ 7**

**Odpowiedzialność Podmiotu przetwarzającego**

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy i przepisami prawa, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych.
3. Podmiot przetwarzający ponosi odpowiedzialność za wszelkie szkody majątkowe lub niemajątkowe poniesione przez osoby trzecie wskutek przetwarzania danych osobowych w sposób naruszający obowiązujące przepisy o ochronie danych osobowych lub Umowę.

**§ 8**

**Czas obowiązywania umowy**

1. Niniejsza umowa obowiązuje od dnia ………………do dnia…………………………… r.
2. W każdym wypadku niniejsza umowa przestaje wiązać Strony, z dniem z którym przestają być związane postanowieniami umowy o której mowa w § 2 ust. 1.

**§ 9**

**Zasady zachowania poufności**

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne”).
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora danych w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

**§ 10**

**Postanowienia końcowe**

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach po jednym egzemplarzu dla każdej ze stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
3. Spory o charakterze sprawy cywilnej mogące wyniknąć na tle realizacji Umowy, Strony poddają jurysdykcji sądów polskich, zaś w zakresie właściwości miejscowej właściwemu rzeczowo sądowi właściwemu dla siedziby Administratora.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Administrator danych Podmiot przetwarzający