

Data Use and Processing Policy

PURPOSE

As a global registry of hematopoietic cell transplant (HCT), cellular therapy (CT) and regenerative medicine (RM) data, the Center for International Blood and Marrow Transplant (CIBMTR) recognizes its responsibility to securely process the data it collects and to use it in compliance with global regulatory requirements. The CIBMTR will maintain a Data Use and Processing Policy (“Policy”) ensuring consistent management of data use and processing procedures.

OBJECTIVE

To establish the practices, including compliance with federal and international regulations, of safeguarding and protecting CIBMTR data use and processing.

SCOPE

This policy applies to CIBMTR staff and may extend to other entities and persons by way of agreements and contracts.

PRINCIPLES

1. CIBMTR shall collect, access, use, store, process, disclose and dispose of data in compliance with all applicable laws, regulations, and standards to ensure data accuracy, validity, safeguarding and protection.
2. Governance and management oversight will occur to ensure CIBMTR processes and controls are suitably designed and effective. CIBMTR will ensure compliance with this policy.
3. CIBMTR shall implement appropriate technical, physical, administrative and organizational measures to protect against unauthorized or unlawful processing and accidental loss and destruction of data. Information security safeguards will at a minimum meet accepted industry best practices. Protective measures will include anonymization and pseudonymization (de-identification) of personal data and integrity and resilience of information systems and services.
4. CIBMTR shall recognize data subject rights, provide notice of data privacy and protection, respond to data requests promptly, and act on data subject requests within the extent of the law.

5. CIBMTR ensures all data under its responsibility is used according to regulatory requirements:
 - Lawfully, fairly and in a transparent manner in relation to the data subject;
 - Collected only for specific, legitimate purposes;
 - Adequately, relevantly and limited to what’s necessary in relation to the purpose for collecting and processing;
 - Kept accurate and up to date;
 - Stored only as long as necessary as defined by the program; and
 - In a manner that ensures appropriate security, integrity and confidentiality.

6. CIBMTR is acknowledged as a Scientific Research Organization and subject to the necessary conditions and safeguards so far as such rights are likely to render impossible or seriously impair the achievement of its scientific research purpose. (GDPR Article 89).

DEFINITIONS

Term / Abbreviation	Meaning
Anonymization	A process where all personally identifying information is removed and it is not possible to link information to a person.
Data Subject	Individual for whom the data pertains
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability Assurance Act
HRPP	Human Research Protection Program
HRSA	Health Resource Services Administration
IRB	Institutional Review Board
OHRP	Office of Human Research Protection
Personal Data	Any information relating to an identified or identifiable natural person (“Data Subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. For the purposes herein, Personal Data may include Special Category Data.
Pseudonymization	De-identification or information where a person is not directly identifiable and there is no reasonable way to identify the person
PII	Personally identifiable information
MHA	Master Healthcare Data and Sample Submission Agreement
PHI	Protected Health Information
DUA	Data Use Agreement

RESPONSIBILITIES

It is the responsibility of each CIBMTR staff member to review, understand and comply with this Policy.

The CIBMTR, in collaboration with the Medical College of Wisconsin (MCW) and the National Marrow Donor Program (NMDP)/Be The Match are responsible for adhering to the Policy. Each operational area’s Senior Leader, or such person’s designee must:

- Implement data release practices to make this Policy operational;
- Educate staff within the functional area in understanding data use and processing procedures;
- Ensure data is used and processed per applicable agreement terms;
- Release only anonymized, de-identified or limited datasets that are compliant with applicable laws and regulations.

APPLICABILITY

The CIBMTR manages a large cellular therapy research database and is a unique information resource for clinicians, researchers and the public interested in Hematopoietic Cell Transplant, Cellular Therapy and Regenerative Medicine. The CIBMTR provides maximum access to and use of its data and operates within the requirements of global regulations. This Policy on data use and processing specifically applies to the requirements of the following human and data protection rules and regulations:

- US Privacy Act
- HIPAA, US
- OHRP, US
- GDPR (see Appendix A), European Union

IMPLEMENTATION

1. CIBMTR will follow its standard policies and procedures regarding data collection and management, including those specific to data protection and safety, access and sharing including but not limited to:
 - (a) Use Personal Data only as necessary for the performance of its obligations under the Master Healthcare Data and Sample Submission Agreement;
 - (b) Ensure that access to the Personal Data is limited to only those staff members who have a legitimate business purpose to access the Personal Data and that all personnel who have access to and/or use Personal Data are obliged to keep the Personal Data confidential;
 - (c) Maintain complete and accurate records of any use of Personal Data it carries out to demonstrate its compliance with the Master Healthcare Data and Sample Submission Agreement;
 - (d) Assist Center in responding to any request from a Data Subject and in ensuring compliance with its obligations to all Data Protection regulations with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;
 - (e) Notify Center without undue delay of becoming aware of any Personal Data breach; such notice to include all information reasonably required by Center to comply with reporting obligations under Data Protection regulations;
 - (f) Promptly notify Center of any communication from a Data Subject regarding the processing of their Personal Data, or any other communication (including from a regulatory authority) relating to either Party's obligations under the Data Protection regulation in respect of the Personal Data;
 - (g) Employ ongoing oversight to the privacy and security obligations to ensure that internal controls are suitably designed and operating effectively to protect against reasonably foreseeable risks to the data, including, but not limited to, auditing of

the privacy and security safeguards based on recognized industry best practices. Upon Center's request, no more than annually, CIBMTR may provide evidence that management oversight has occurred. Such evidence should briefly describe the oversight process, indicate whether CIBMTR's controls remain aligned to industry best practices, and include a signature of a corporate officer of the CIBMTR;

- (h) Assign a qualified data protection officer, or information security official, when core use activities include large-scale genetic, ethnic or racial personal information meeting relevant requirements.
- (i) Not transfer any Personal Data across international borders unless the following conditions are fulfilled:
 - 1. A Party has provided appropriate safeguards in relation to the transfer;
 - 2. The Data Subject has enforceable rights and effective legal remedies; and
 - 3. The Party acting as Data Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; and
- (j) At the written direction of Center, inactivating Personal Data on termination or expiration of the Master Healthcare Data and Sample Submission Agreement unless such Personal Data is allowed to be maintained by applicable law.

2. Rules and Regulations

Institutions submitting data to the CIBMTR are expected to comply with their country's laws and regulations governing human subjects and privacy protection, and to obtain explicit individual consent to data submission.

In the U.S., the CIBMTR operates as a Public Health Authority (PHA) as the contractor for the Stem Cell Therapeutic Outcomes Database (SCTOD) under the Stem Cell Act of 2005 (renewed 2010 and 2015) for the collection of stem cell transplant data and, as such, data relevant to the SCTOD may be disclosed by centers without direct patient consent. Any data that lacks consent may be used in furtherance of public health matters outlined in the SCTOD and is excluded from all other uses.

The CIBMTR uses, processes and releases data as anonymized, de-identified and limited datasets that comply with all relevant rules and regulations regarding privacy and confidentiality as described in the following table.

Regulation / Rule / Country	(De)Identification Definition																				
<p>GDPR European Union Source: https://fpf.org/wp-content/uploads/2016/11/M-Hintze-GDPR-Through-the-De-Identification-Lens-31-Oct-2016-002.pdf</p>	<p>An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location number, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.</p> <p>De-identification may relate to a specific person whose identity is not apparent from the data; and the data is not directly linked with data that identifies the person. The data could potentially be re-identified if matched to additional identifying data provided by the data subject, there is no systematic way for the controller to reliably create or re-create a link with identifying data.</p> <p>Anonymous/Aggregate data is: 1.) stored without identifiers or other data that could identify the individual or device to whom the data relates; and 2.) aggregated with data about enough individuals such that it does not contain individual-level entries or events linkable to a specific person. Anonymization methods must be irreversible and eliminate any known or foreseeable possibility of linking any of the data to an individual to who the data originally related.</p> <p>The four levels may be summarized as follows:</p> <table border="1" data-bbox="561 970 1408 1276"> <thead> <tr> <th></th> <th>Identified</th> <th>Identifiable</th> <th>Article 11 De-identified</th> <th>Anonymous/Aggregate</th> </tr> </thead> <tbody> <tr> <td>Directly linked to identifying data</td> <td>Yes</td> <td>No</td> <td>No</td> <td>No</td> </tr> <tr> <td>Known, systematic way to (re)identify</td> <td>Yes</td> <td>Yes</td> <td>No</td> <td>No</td> </tr> <tr> <td>Relates to a specific person</td> <td>Yes</td> <td>Yes</td> <td>Yes</td> <td>No</td> </tr> </tbody> </table> <p>Each greater level of de-identification provides more protection and further reduces risk to individuals. The first three levels all are personal data within the scope of European data protection law, including ten levels with meaningful distinctions between each.</p>		Identified	Identifiable	Article 11 De-identified	Anonymous/Aggregate	Directly linked to identifying data	Yes	No	No	No	Known, systematic way to (re)identify	Yes	Yes	No	No	Relates to a specific person	Yes	Yes	Yes	No
	Identified	Identifiable	Article 11 De-identified	Anonymous/Aggregate																	
Directly linked to identifying data	Yes	No	No	No																	
Known, systematic way to (re)identify	Yes	Yes	No	No																	
Relates to a specific person	Yes	Yes	Yes	No																	
<p>HIPAA US</p>	<p>The HIPAA defined identifiers are listed below. De-identified data will have all (any) identifiers removed or coded so that they cannot be linked back to an individual.</p> <ul style="list-style-type: none"> • Name; • Street address, city, county, precinct, or zip code (unless only the first three digits of the zip code are used, and the area has more than 20,000 residents); • The month and day of dates directly related to an individual, such as birth date, admission date, discharge date, dates of service, or date of death; • Age if over 89 (unless aggregated into a single category of age 90 and older); 																				

Regulation / Rule / Country	(De)Identification Definition
	<ul style="list-style-type: none"> • Telephone numbers; • Fax numbers; • Email addresses; • Social security numbers; • Medical record numbers; • Health plan beneficiary numbers; • Account numbers; • Certificate/license numbers; • Vehicle identifiers, serial numbers, and license plate numbers; • Device identifiers and serial numbers; • Web Universal Resource Locators (URLs) and Internet Protocol (IP) addresses; • Biometric identifiers, such as fingerprints; • Full-face photographs and any comparable images; or • Any other unique identifying number, characteristic, or code.
<p>OHRP US</p>	<p>OHRP does not consider data to be individually identifiable if the data cannot be linked to a specific individual by the investigator either directly or indirectly through coding systems. If the two conditions below are both met, OHRP does not consider the research using this data to involve human subjects:</p> <ol style="list-style-type: none"> 1. The private information or specimens were not collected specifically for the currently proposed research project through an interaction or intervention with living individuals and; 2. The investigator(s) cannot readily ascertain the identity of the individual(s) whom the coded private information or specimens pertain because, for example: <ol style="list-style-type: none"> a. The investigator(s) and the holder of the key entered into an agreement prohibiting the release of key to the investigator(s) under any circumstances, until the individual(s) are deceased (note that the HHS regulations do not require the IRB to review and approve this agreement); b. There are IRB-approved written policies and operating procedures for a repository or data management center that prohibit the release of the key to the investigator(s) under any circumstances, until the individual(s) are deceased; or c. There are other legal requirements prohibiting the release of the key to the investigators, until the individual(s) are deceased. <p>Data compiled by CIBMTR from the CIBMTR Research Database for specific research projects meet these two conditions.</p> <p>Condition 1: All data were collected as part of the Research Database protocol and not for the specific research project for which the data set is being compiled.</p>

Regulation / Rule / Country	(De)Identification Definition
	<p>Condition 2: CIBMTR is bound by federal regulations to not disclose the identity of any participant in the Stem Cell Therapeutic Outcomes Database and is bound by CIBMTR internal policies and SOPs to not release the identity of any participant in the Research Database.</p> <p>When data satisfy these two conditions, IRB approval at the investigator's institution is not required by the federal regulations pertaining to human research subject protection.</p>
<p>US Privacy Act, 1974</p>	<p>The Privacy Act of 1974, a United States federal law, establishes a Code of Fair Information Practice that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual. The Privacy Act requires that agencies give the public notice of their systems of records by publication in the Federal Register. The Privacy Act prohibits the disclosure of information from a system of records absent of the written consent of the subject individual, unless the disclosure is pursuant to one of twelve statutory exceptions. The Act also provides individuals with a means by which to seek access to and amendment of their records and sets forth various agency record-keeping requirements. Additionally, with people granted the right to review what was documented with their name, they are also able to find out if the "records have been disclosed" and are also given the rights to make corrections.</p>

3. Human Research Protection Program

The CIBMTR works with NMDP/Be The Match to maintain a comprehensive Human Research Protection Program (HRPP) to ensure that the rights and welfare of participants in its research are protected and to ensure compliance with all pertinent US federal regulations. The NMDP/Be The Match Human Research Protection Program is accredited by the Association for the Accreditation of Human Research Protection Programs (AAHRPP). Under an Institutional Review Board (IRB) Authorization Agreement between MCW and NMDP/Be The Match, the NMDP IRB serves as the IRB of record for all research conducted by the CIBMTR. The NMDP IRB has the authority to approve, require modifications in, or disapprove all research activities within its jurisdiction as specified by both federal and state regulations and NMDP/Be The Match policies and procedures. As part of the CIBMTR human research protection program, all CIBMTR staff members are required to complete initial and continuing education and training in the protection of human subjects through the Collaborative Institutional Training Initiative (CITI).

4. Data Privacy

The CIBMTR is obligated to securely handle Protected Health Information (PHI). Unless otherwise indicated and approved by a CIBMTR Senior Leader, datasets released to non-government entities are de-identified with respect to patient, donor and center identifiers. In special circumstances in which a data set is requested that may involve private or PHI that could identify a patient, or center, a specific confidentiality agreement and DUA will be executed, after consideration by the CIBMTR Senior Leaders. Such research must be approved by an IRB prior to initiation.

- For the majority of studies/projects, CIBMTR staff follow a standard procedure for creation of anonymized, pseudonymized or de-identified datasets that specifies removal of all patient, donor, and center identifiers, which could lead to the identification of a patient or transplant center from data files.
- The CIBMTR will not release identifiable patient or center variables unless these data are critical to the approved study / project or will be used for linking to another data file via an established honest broker relationship. In these cases where a limited data set is provided, special procedures are outlined in the *Linking CIBMTR Data to External Databases or Data Sources Standard Operating Procedure* and documented with CIBMTR's Data Use Agreement (DUA), the *Letter of Commitment to Complete CIBMTR Observational Studies*, and established prior to final approval of the request.
- In cases of an approved study or project or when datasets are requested from previous research, the requestor must submit a DUA that specifies the requirements for using the CIBMTR data before final approval of the project is offered. The DUA is provided when a study protocol or statement of work has been submitted and associates the proposed use of the data with the DUA.

Note: The CIBMTR DUA specifies commitment from the investigator and their institution to protection of privacy, prevention of unauthorized sharing of data or attempts to re-identify centers or patients (unless previously authorized to do so), data retention periods or destruction of datasets at the completion of the proposed work (where relevant).

5. Proprietary Data

The CIBMTR shares data with the private sector (e.g., pharmaceutical and biotechnology clients). Temporary data restrictions may be applied by a private sector client agreement due to co-funding terms and intellectual property rights. Any such restrictions will be outlined in a Rider of the Master Healthcare Data and Sample Submission Agreement (MHA). The CIBMTR is committed to data transparency with intent to share data to support the scientific community and public interest. Any agreement to data restriction will be reviewed at the time of request and held to a minimum. The CIBMTR recognizes journal restrictions to data release and will comply with those restrictions.

Restrictions are documented in the written data request and disclosed as needed.

6. Methods for Data Sharing

Release of data follows the terms described in the *CIBMTR Data Release Policy* and the *CIBMTR MS Biostatistician Reference Guide* in conjunction with the *Data Sharing to Non-CIBMTR and Non-NMDP Employees SOP* enables accurate and efficient data selection, de-

identification and dataset approval. Datasets are only shared through secure file sharing solutions that are limited to a minimum number of key personnel involved in the project.

7. Data Security

Data submitted to CIBMTR is protected by safeguards ensuring security and stringent access control as described in its Standard Operating Procedures. The CIBMTR uses standard security practices and controls to protect data; maintains a System Security Plan of management, operational and technical controls; and undergoes an annual information security assessment by a qualified, independent third party. CIBMTR follows the National Institute of Standards and Technology (NIST 800-53) information security framework. CIBMTR data systems are maintained in accordance with the US Federal Information Systems Management Act of 2002, the U.S. Health Resources & Services Administration, and the General Data Protection Regulation, “GDPR” (Regulation EU 2016/679).

8. Section 508 Compliance

Public data is posted on the [HRSA](#) website and these data are certified Section 508 compliant per a completed VPAT (Voluntary Product Accessibility Template).

References

Country / Global Entity	Regulation/ Standard
US	Office of Human Research Protection (OHRP) common rule regulations (45CFR Part 46)
US	Health Insurance Portability and Accountability Act (HIPAA) privacy rule (45 CFR Part 160)
US	US Privacy Act 1974, (<u>Privacy Act of 1974, 5 U.S.C. § 552a</u>)
US	Office of Management and Budget (OMB) Circular No. A-130 <i>Managing Information as a Strategic Resource.</i>
US	National Institute of Standards and Technology (NIST) Special Publication 800-18, <i>Guide for Developing Security Plans for Information Technology Systems.</i>
US	National Institute of Standards and Technology (NIST) Special Publication 800-53, <i>Security Controls and Assessment Procedures for Federal Information Systems and Organizations.</i>
European Union	General Data Protection Regulation (GDPR) (EU 2016/679)

Addenda

Appendix A - GDPR

APPENDIX A – GDPR

CIBMTR recognizes and is compliant with GDPR requirements as detailed in the following table.

GDPR Specific Definitions and Acronyms

Term / Abbreviation	Meaning
Data Co-Controller	Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers.
Data Controller	The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of Personal Data; where the purposes and means of processing are determined by European Union (EU) or Member State laws, the controller may be designated by those laws.
Data Processor	A natural or legal person, public authority, agency or any other body which processes Personal Data on behalf of the controller.
Data Protection Legislation	All applicable legislation protecting the Personal Data of natural persons, including: (i) the Data Protection Act 1998; (ii) GDPR; and (iii) any successor legislation to the GDPR or the Data Protection Act 1998, together with binding guidance and codes of practice issued from time to time by relevant supervisory authorities.
Processing	Any operation or set of operations performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
Special Category Data	Any data that reveals: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data for the purpose of uniquely identifying a natural person; and data concerning health or a natural person's sex life and/or sexual orientation.
Standard Contractual Clauses	The contractual clauses set out in Schedule 3, amended as indicated in that Schedule.
Restricted Transfer	Any transfer of Personal Data that would be prohibited by the Data Protection Legislation in the absence of the Standard Contractual Clauses.
EEA	European Economic Area. The EEA includes EU countries and also Iceland, Liechtenstein and Norway.
Schedule 2	Details of the processing of Personal data as required by Article 28(3) GDPR (or equivalent provisions of any Data Protection Legislation).

Term / Abbreviation	Meaning
Schedule 3	Standard Contractual Clauses (Processors) for the purposes of Article 26(2) of Directive 95/46/EC established in third countries which do not ensure an adequate level of data protection.

Purpose: For the purposes of the Data Protection Legislation, CIBMTR and Center shall be Data Co-Controllers. These data use and processing requirements set out in the CIBMTR Policy, and as described in Standard Contractual Clauses Schedule 2 and Schedule 3 provided in reference for sharing of Personal Data between the Parties as Data Co-Controllers. The CIBMTR is also acknowledged as a Scientific Research Organization and, pursuant to the Article 89, is applicable for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the necessary conditions and safeguards so far as such rights are likely to render impossible or seriously impair the achievement of its scientific research purpose.

- 1.1 CIBMTR requires access to certain Personal Data to conduct scientific/medical research and fulfill its domestic regulatory requirements to report outcomes of products infused for certain therapies and other regulatory reporting requirements for drug and devices to Regulatory Agencies.
- 1.2 It is recognized that there are significant benefits to both CIBMTR and the Center having this relationship and exchanging such information. This Policy ensures that where Personal Data may be provided or accessed, such provision and subsequent use and maintenance will at all times comply with the requirements herein and the GDPR.
- 1.3 The sharing of Personal Data is necessary to support the following purposes of both CIBMTR and Center:
 - (a) Conduct research on hematopoietic cell transplantation (HCT), cellular therapies and marrow toxic injuries;
 - (b) Report outcomes of HCT recipients of a US donor product as required by United States regulatory requirements; and
 - (c) Regulatory reporting for drug and devices to regulatory agencies and manufacturers.
- 1.4 CIBMTR's data processing requirements and its Master Healthcare Data and Sample Submission Agreement formalizes a lawful transfer of Personal Data between the Parties and presents no new or additional privacy concerns.
- 1.5 CIBMTR will not process Personal Data in a way that is incompatible with its Data Use and Processing Policy.

2. Overarching Data Protection Requirements.

- 2.1 **Internal Procedures and Safeguards.** CIBMTR has implemented appropriate technical, physical, administrative, and organizational measures, to protect against unauthorized or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, appropriate to the harm that might result from the unauthorized or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of

technological development and the cost of implementing any measures. Those measures may include, where appropriate, anonymizing and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of measures adopted by it. At the very least, CIBMTR and Center shall have safeguards that are no less rigorous than accepted industry best practices, including the International Organization for Standardization's standards: ISO/IEC 27001:2013 (or any successor) – Information Security Management Systems, and shall ensure that all such safeguards, including the manner in which Personal Data is collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions herein.

- 2.2 Compliance with Data Protection Legislation. CIBMTR complies with all applicable requirements of the Data Protection Legislation and ensure that any of their staff involved with the activities shall comply.
- 2.3 CIBMTR acknowledges the right to audit activities if required by the center. CIBMTR also acknowledges that the competent authority or authorities has the right to inspect its activities, including on-site inspections, should it wish to do so as part of its inspection of the other Party; provided, however, that information and audit rights of one Data Co-Controller only arise under this section to the extent that the other Data Co-Controller does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, Article 28(3)(h) of the GDPR).

3. **Shared Personal Data.** For the purposes of the Purposes listed in Section 2.4 above, the following types of Personal Data to be shared include: demographic data (first and last name, address, birthdate and birth location, mother's maiden name (optional), ethnicity and race); genetic data, health information (disease, lab results, drugs, outcomes of HCT, cellular therapies and marrow toxic injuries); and socioeconomic data (marital status, occupation, work status, education, health insurance).

- 3.1 Anonymization. CIBMTR agrees, as far as reasonably practical, to either anonymize or pseudonymize all Personal Data shared.

4. **Data Co-Controller Responsibilities.**

- 4.1 Center Co-Controller Responsibilities. Center is expected to be responsible for the following obligations:
 - (a) Ensuring that it has all necessary consents and notices in place to lawfully collect, process and transfer Personal Data to CIBMTR. Such consent and notices must provide clear and sufficient information to Data Subjects in order for them to understand what of their Personal Data the Parties are sharing, the circumstances in which it will be shared, the purposes for the

data sharing, how their Personal Data will be processed, and the identity of the organization that is receiving the Personal Data;

- (b) Acting as the primary point of contact for Data Subjects generally and for purposes of allowing Data Subjects to enforce their rights under GDPR;
- (c) Assigning a qualified data protection officer when core processing activities include large scale processing of genetic, ethnic or racial personal information meeting the relevant requirements of Data Protection Law (including, where applicable, Article 37);
- (d) Ensuring that the rights of the Data Subject (enumerated in Articles 12-23 of GDPR, to the extent that they apply) are met. Where Center requires the assistance of CIBMTR to enable them to comply with Data Subject access requests and/or other inquiries or complaints, CIBMTR agrees to provide Center with reasonable and prompt assistance; and
- (e) Ensuring the security of transmission of any Personal Data to CIBMTR.

4.2 CIBMTR Co-Controller Responsibilities. CIBMTR will follow its standard policies and procedures regarding data collection and management, including those specific to data protection and safety, access and sharing. It will be responsible for the following obligations:

- (a) Processing Personal Data only as necessary for the performance of its obligations under the Master Healthcare Data and Sample Submission Agreement;
- (b) Ensuring that access to the Personal Data is limited to only those staff members who have a legitimate business purpose to access the Personal Data and that all personnel who have access to and/or process Personal Data are obliged to keep the Personal Data confidential;
- (c) Maintaining complete and accurate records of any processing of Personal Data it carries out to demonstrate its compliance with the Master Healthcare Data and Sample Submission Agreement;
- (d) Assisting Center, in responding to any request from a Data Subject and in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;
- (e) Notifying Center without undue delay of becoming aware of any Personal Data breach, such notice to include all information reasonably required by Center to comply with reporting obligations under Data Protection Legislation;
- (f) Promptly notifying Center of any communication from a Data Subject regarding the processing of their Personal Data, or any other communication (including from a supervisory authority) relating to either Party's obligations under the Data Protection Legislation in respect of the Personal Data;

- (g) Employing ongoing oversight to the privacy and security obligations to ensure that internal controls are suitably designed and operating effectively to protect against reasonably foreseeable risks to the data, including, but not limited to, auditing of the privacy and security safeguards based on recognized industry best practices. Upon Center's request, no more than annually, CIBMTR must provide evidence that management oversight has occurred. Such evidence should briefly describe the oversight process, indicate whether CIBMTR's controls remain aligned to industry best practices, and include a signature of a corporate officer of the CIBMTR;
- (h) Assigning a qualified data protection officer when core processing activities include large scale processing of genetic, ethnic or racial personal information meeting the relevant requirements of Data Protection Law (including, where applicable, Article 37);
- (i) Not transferring any Personal Data across international borders unless the following conditions are fulfilled:
 - (1) A Party has provided appropriate safeguards in relation to the transfer;
 - (2) The Data Subject has enforceable rights and effective legal remedies; and
 - (3) The Party acting as Data Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; and
- (j) At the written direction of Center, inactivating, deleting or returning Personal Data and copies thereof to Center on termination or expiration of the Master Healthcare Data and Sample Submission Agreement unless such Personal Data is allowed to be maintained by applicable law.

4.3 Sub-Processing. CIBMTR is granted general pre-authorization to use third-party data processing services so long as all obligations set forth herein are applied to the third-party (specifically including sub-sections (a) and (b) below). CIBMTR shall:

- (a) Enter into a written agreement with the third-party processor that incorporates terms which offer at least the same level of protection for the Personal Data as those set out herein and which meet the requirements of Article 28 of the GDPR; and
- (b) If such an arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the written agreement referred to in clause 2.4(a) above.

4.3.1 Liability for Sub-Processor. CIBMTR shall, to the extent it does not transfer liability to the sub-processor, remain fully liable for all acts or omissions of any third-party processor it appoints.

4.3.2 Indemnification. Each Co-Controller is responsible for its own negligent acts with respect to use of the data.

5. **Resolution of Disputes with Data Subjects or the Data Protection Authority.** In the event of a dispute or claim brought by a Data Subject or the Data Protection Authority concerning the processing of Personal Data against either or both Parties, the Parties will inform each other about any such disputes or claims and will cooperate with a view to settling them amicably and in a timely fashion. The Parties may participate in any proceedings required by a dispute or claim remotely, such as by telephone or other electronic means.

Model Contractual Clauses

Clause 1 **Definitions**

For the purposes of the Clauses:

- (a) 'Personal Data', 'special categories of data', 'process/processing', 'controller', 'processor', 'Data Subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data;
- (b) 'The data exporter' means the controller who transfers the Personal Data;
- (c) 'The data importer' means the processor who agrees to receive from the data exporter Personal Data for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- (d) 'The sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer Personal Data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) 'The applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of Personal Data applicable to a Data Controller in the Member State in which the data exporter is established;
- (f) 'Technical and organizational security measures' means those measures aimed at protecting Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2
Details of the transfer

The details of the transfer and in particular the special categories of Personal Data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3
Third-Party beneficiary clause

1. The Data Subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-Party beneficiary.

2. The Data Subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the Data Subject can enforce them against such entity.

3. The Data Subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the Data Subject can enforce them against such entity. Such third-Party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The Parties do not object to a Data Subject being represented by an association or other body if the Data Subject so expressly wishes and if permitted by national law.

Clause 4
Obligations of the data exporter

The data exporter agrees and warrants:

(a) That the processing, including the transfer itself, of the Personal Data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) That it has instructed and throughout the duration of the Personal Data processing services will instruct the data importer to process the Personal Data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) That the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 to this contract;

(d) That after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) That it will ensure compliance with the security measures;

(f) That, if the transfer involves special categories of data, the Data Subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) To forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) To make available to the Data Subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) That, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the Personal Data and the rights of Data Subject as the data importer under the Clauses; and

(j) That it will ensure compliance with Clause 4(a) to (i).

Clause 5
Obligations of the data importer

The data importer agrees and warrants:

(a) To process the Personal Data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) That it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data

exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) That it has implemented the technical and organisational security measures specified in Appendix 2 before processing the Personal Data transferred;

(d) That it will promptly notify the data exporter about:

(i) Any legally binding request for disclosure of the Personal Data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) Any accidental or unauthorised access, and

(iii) Any request received directly from the Data Subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) To deal promptly and properly with all inquiries from the data exporter relating to its processing of the Personal Data Subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) At the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) To make available to the Data Subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the Data Subject is unable to obtain a copy from the data exporter;

(h) That, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) That the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) To send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6 **Liability**

1. The Parties agree that any Data Subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any Party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a Data Subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the Data Subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the Data Subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a Data Subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the Data Subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the Data Subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7
Mediation and jurisdiction

1. The data importer agrees that if the Data Subject invokes against it third-Party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the Data Subject:

- (a) To refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
- (b) To refer the dispute to the courts in the Member State in which the data exporter is established.

2. The Parties agree that the choice made by the Data Subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8
Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The Parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9
Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10
Variation of the contract

The Parties undertake not to vary or modify the Clauses. This does not preclude the Parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11
Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-Party beneficiary clause as laid down in Clause 3 for cases where the Data Subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-Party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of Personal Data processing services

1. The Parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the Personal Data transferred and the copies thereof to the data exporter or shall destroy all the Personal Data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the Personal Data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the Personal Data transferred and will not actively process the Personal Data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.