POLICY

PURPOSE

As a global registry of hematopoietic cell transplant (HCT) and other adoptive cellular therapy (ACT) data, and Gene Therapies (GT), together cellular therapy 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 regarding privacy and confidentiality. The CIBMTR will maintain a Data Use and Processing Policy ("Policy") ensuring consistent management of data use and processing procedures.

This Policy shall establish the practices, including compliance and alignment with United States (US) and international regulations, for safeguarding and protecting data during processing and use.

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, disclosure, loss and destruction of data. Information security safeguards will at a minimum meet accepted industry best practice. Protective measures will include anonymization and pseudonymization (de-identification) of PII / 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;
    - Is minimized only to that which will provide current and potential scientific research value;

- 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, ACRONYMS AND ABBREVIATIONS

Term	Meaning
ACT	Adoptive Cellular Therapy
Anonymization	A process where all personally identifying information is removed and it is not possible to link information to a person.
Cellular Therapy Data	All data associated with use of cellular therapies including HCT as well as genetically modified cells including chimeric antigen receptors (CAR)-T and Gene Therapies
CIBMTR	The Center for International Blood and Marrow Research (CIBMTR) is an affiliated research program established as a collaboration between MCW and the National Marrow Donor Program®/Be The Match® (“NMDP”)
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. See below for additional definitions.
Data Subject	Individual for whom the data pertains
Deidentified data	All (any) identifiers removed or coded in such a way that they cannot be linked back to an individual
DUA	Data Use Agreement
GDPR	General Data Protection Regulation
GT	Gene Therapy
HCT	Hematopoietic Cell Transplantation
Healthcare clearinghouse	An entity that processes or facilitates the processing of healthcare transactions. Act as an intermediary between healthcare providers and health plans, ensuring that data is transmitted correctly and efficiently.
HIPAA	Health Insurance Portability Assurance Act of 1996
Honest Broker	A neutral intermediary that collects and provides de-identified patient data. Ensures the data is stripped of any identifiable information and cannot be traced back to individual patients.
HRPP	Human Research Protection Program
HRSA	Health Resource Services Administration
IRB	Institutional Review Board
Limited Dataset	A collection of data that is stripped of personal identifiers to protect privacy, while still retaining enough information to be useful in analyses. Limited datasets may include some identifiable information (date(s), geographic details, etc.), but lack critical direct data elements (name, address, etc.). Access to a limited dataset generally requires a data use agreement (DUA) to ensure it is only used for research purposes.

MHA	Master Healthcare Data and Sample Submission Agreement; a standalone Agreement that replaces the Data Transmission Agreement (DTA) and covers the mandated reporting under the C.W. Bill Young Cell Transplantation Program, https://bloodcell.transplant.hrsa.gov/about/, as well as the *Data/Samples* with Informed Consent submitted under CIBMTR Protocols with https://www.cibmtr.org/DataManagement/ProtocolConsent/Pages/index.aspx
OHRP	Office of Human Research Protection
PHA	Public Health Authority
PHI	Protected Health Information: a subset of PII protected by HIPAA PII related to one's health or used in a healthcare context is considered PHI and governed by HIPAA.
PI	Principal Investigator
PII and 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, 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. Any information about an individual maintained by an agency, that can be used to identify an individual, directly or indirectly, by reference to an identifier. Definitions of PII/Personal Data differ by governance. See Appendix A for definitions and further information. Examples of PII identifiers: • Patient name(s) • Geographical elements (street address, city, county, zip code) • Dates related to the health or identity of individuals (including birthdays, date of admission, date of discharge, date of death, or exact age of a patient older than 89) • Telephone numbers • Fax numbers • Email addresses • Social Security numbers • Medical record numbers • Health insurance beneficiary numbers • Account numbers • Certificate/license numbers • Vehicle identifiers • Device attributes or serial numbers • Digital identifiers, such as website URLs • IP addresses • Biometric elements, including finger, retinal, and voiceprints • Full face photographic images

	• Other identifying numbers/codes The European Union GDPR specifies an identifiable natural person as one who can be identified, directly or indirectly, 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. OHRP does not have a separate, formal definition of personal data distinct from its understanding of PII. Both PII and personal data according to OHRP refer to any information that relates to an identified or identifiable information. Examples according to OHRP include: • Name • Contact details (address, email, phone number) • Identification numbers (Social Security number) • Biographical details (date of birth, gender, etc.) • Health information and records • Biometric data • Genetic data, and • Any other data that can be linked to an individual
PII	Personally identifiably information
Pseudonymization	De-identification or information where a person is not directly identifiable and there is no reasonable way to identify the person
SCTOD	Stem Cell Therapeutic Outcomes Database
US	United States
VPAT	Voluntary Product Accessibility Template

RESPONSIBILITIES

It is the responsibility of each CIBMTR staff member to review, understand and comply with this Policy. The CIBMTR, within the Medical College of Wisconsin (MCW) and NMDP 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

CIBMTR manages a large research database and is a unique information resource for clinicians, researchers and the public interested in Hematopoietic Cell Transplant (HCT), other Cellular Therapy and Gene Therapies. 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 B), European Union, and
- other international regulations that have similarities to GDPR

CIBMTR collects personally identifiable information (PII) as part of the data registry operations. The types of PII collected may include, but are not limited to, donor information, center information, patient attributes, and other identifiers necessary for the purposes of the registry.

While CIBMTR collects and maintains PII and adheres to the Health Insurance Portability and Accountability Act, it is important to note that CIBMTR, as a research organization, does not engage in activities classifying the organization as a HIPAA covered entity, such as transmitting, processing, or storing protected health information (PHI) for healthcare providers, health plans, or healthcare clearinghouses. CIBMTR is not a covered entity and HIPAA regulations are not specifically required.

CIBMTR adheres to the US Privacy Act, HIPAA's Privacy Rule, and the OHRP regarding authorizations to use and disclose PHI for research. CIBMTR is committed to ensuring that all PII is handled with the highest standards of data privacy and security. This includes implementing appropriate technical and administrative safeguards to protect the data we collect. CIBMTR remains in compliance with other applicable data registry regulations, to include General Data Protection Regulation (GDPR).

If transferring personal data to a third country, CIBMTR will verify, on a case-by-case basis, if there is anything in the law and practice of the third country which may impinge on the appropriate safeguards of the transfer tools/process. If the law and practice of the third country do impinge the transfer tools safeguards, CIBMTR will implement supplementary measures to ensure an equivalent level of protection.

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 PII/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 PII/Personal Data is limited to only those staff members who have a legitimate business purpose to access the PII/Personal Data and that all personnel who have access to and/or use PII/Personal Data are obliged to keep the PII/Personal Data confidential;
    (c) maintain complete and accurate records of any use of PII/Personal Data it carries out to demonstrate its compliance with the Master Healthcare Data and Sample Submission Agreement;
    (d) assist Centers 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 Centers without undue delay of becoming aware of any PII/Personal Data breach; such notice to include all information reasonably required by Centers to comply with reporting obligations under Data Protection regulations;

(f) promptly notify Centers of any communication from a Data Subject regarding the processing of their PII/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 PII/Personal Data;

(g) employ ongoing oversight to the privacy and security obligations to assess privacy risk to individuals and 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 or disclose any PII/Personal Data across international borders unless the following conditions are fulfilled:

- a Party has provided appropriate safeguards in relation to the transfer;
- the Data Subject has enforceable rights and effective legal remedies; and
- the Party acting as Data Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any PII/Personal Data that is transferred; and establish policy and controlled processes for review and approval to disclose limited PII in special circumstances, such as to facilitate computerized matching of data with another data source via honest broker to achieve the aims of an approved study

(j) at the written direction of the center, inactivating PII/Personal Data on termination or expiration of the Master Healthcare Data and Sample Submission Agreement unless such PII/Personal Data is allowed to be maintained by applicable law.

2. Rules and Regulations

Institutions submitting data to 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 (reauthorized 2010 and 2015) for the collection of allogeneic stem cell transplant data and, as such, data relevant to the SCTOD may be disclosed by centers without direct patient consent. Any allogeneic HCT 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 below:

<table>
<tr><th>Regulation/ Rule/ Country</th><th>(De)Identification Definition</th></tr>
<tr><td>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</td><td>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.
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.
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.
The four levels may be summarized as follows:

<table>
<tr><th></th><th>Identified</th><th>Identifiable</th><th>Article 11 De-identified</th><th>Anonymous/ Aggregate</th></tr>
<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>
</table>

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.</td></tr>
<tr><td>HIPAA
US</td><td>HIPAA defined identifiers are listed in Appendix A. De-identified data will have all (any) identifiers removed or coded so that they cannot be linked back to an individual.</td></tr>
<tr><td>OHRP
US</td><td>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</td></tr>
</table>

	consider the research using this data to involve human subjects: 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: 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. Data compiled by CIBMTR from the CIBMTR Research Database for specific research projects meet these two conditions. 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. 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. 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.
US Privacy Act, 1974	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.

3. Human Research Protection Program

NMDP to maintains 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 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, 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 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

CIBMTR is obligated to securely handle PII. Unless otherwise indicated and approved due to an exception that adheres to the CIBMTR PII Disclosure Procedure (**SOP-0100 Approval to Disclose PII for Linking or Computerized Matching Person Data to External Data Sources**), 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 PII 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.

CIBMTR will not release identifiable patient or center variables unless these data are critical to the approved study / project or will be used to facilitate computerized matching 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 **SOP-0100 Approval to Disclose PII for Linking or Computerized Matching Person Data to External Data Sources**, documented with CIBMTR's Data Use Agreement (DUA), and within a letter of commitment signed by the Principal Investigator (PI). The DUA are letter of commitment are 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

CIBMTR shares data with the private sector (e.g., pharmaceutical and biotechnology clients). Temporary data restrictions (data embargos) 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). 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 by Senior Leadership and held to a minimum. 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 this policy**,** the *CIBMTR MS Biostatistician Reference Guide*, and **SOP-0100 Approval to Disclose PII for Linking or Computerized Matching Person Data to External Data Sources**. These methods enable 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 Policies, Guides and Standard Operating Procedures. 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 aligns with 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 of the Rehabilitation Act (29 U.S.C. § 794d) 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

Document	Description
European Union	General Data Protection Regulation (GDPR) (EU 2016/79)
N/A	Health Insurance Portability and Accountability act (HIPAA) Privacy Rule (45 CFR Part 160)
N/A	National Institute of Standards and Technology (NIST) Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*
N/A	National Institute of Standards and Technology (NIST) Special Publication 800-53, *Security Controls and Assessment Procedures for Federal Information Systems and Organizations.*
N/A	Office of Human Research Protection Program (OHRP) common rule regulations (45CFR Part 46)
N/A	Office of Management and Budget (OMB) Circular No. A-130 *Managing Information as a Strategic Resource*
N/A	US Privacy Act 1974, (Privacy Act of 1974, 5 U.S.C. § 552a)
POL-0003	Data Release Policy
SOP-0100	Approval to Disclose PII for Linking or Computerized Matching Person Data to External Data Sources

REVISION HISTORY

Revision	Brief Description
Rev 01	Initial upload to MasterControl (previous reference number QAC P00005)
Rev 02	Removed Contractual Clauses and inserted a link for European Commission website for Standard Contractual Clauses (SCC) to access most up to date information.
Rev 03	Periodic review performed. Human and data protection rules and regulations reviewed. Minor language updates and additional definitions inserted.
Rev 04	Periodic review performed. Updated language in applicability section regarding PII governance.

APPENDICES

Appendix	Title
A	Governance- Definition and Examples of PII/Personal Data
B	GDPR

Appendix A: Governance – Definition and Examples of PII/Personal Data

Governance	Definition of PII / Personal data
GDPR	GDPR defines personal data as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person who can be identified, directly or indirectly, by reference to an identifier. GDPR personal data identifiers: • Name • Identification number • Location number • Online identifier • One or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of a natural person
HIPAA	The definition of PII/personal data according to HIPAA is any information that can be used to identify an individual. HIPAA further breaks PII down into a sub-set of PII related to one's health. HIPAA defined Identifiers: • Patient name(s) • Geographical elements (street address, city, county, and/or zip code) • Dates related to the health or identity of individuals (including birthdays, date of admission, date of discharge, date of death, or exact age or a patient older than 89) • Telephone numbers • Fax numbers • Email addresses • Social Security numbers • Medical record numbers • Health insurance beneficiary numbers • Account numbers • Certificate/license numbers • Vehicle identifiers • Device attributes or serial numbers • Digital identifiers, such as website URLs • IP addresses • Biometric elements, including finger, retinal, and voiceprints • Full face photographic images • Other identifying numbers/codes
OHRP	OHRP refers to information that relates an identified or identifiable information as PII/Personal Data. Examples include: • Name • Contact details (address, email, phone number) • Identification numbers (Social Security)

	• Biographical details (date of birth, gender, etc.) • Health information and health records • Biometric data • Genetic data, and • Any other data that can be linked to an individual
NIST	According to NIST, PII is "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual such as medical, educational, financial, and employment information". Examples include: • Name (full, maiden, mother's maiden, alias) • Personal identification number (SSN, passport, driver's license, taxpayer identification, credit card number, etc.) • Address (street or email) • Asset information (Internet Protocol or Media Access Control) • Telephone numbers • Personal characteristics, including photographic, x-rays, fingerprints, or other biometrics • Information identifying personally owned property (vehicle registration, title number) • Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, geographical indicators, employment information, medical information, education information, financial information)

Appendix B: GDPR

CIBMTR recognizes and is compliant with GDPR requirements as detailed below:

GDPR Specific Definitions and Acronyms Table-

Definitions/Acronyms/ Abbreviations	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).

Definitions/Acronyms/ Abbreviations	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, 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 ensures 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, either remotely or on site, 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 the competent authorities or authorities 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) ensuring the security of transmission of any Personal Data from Center when CIBMTR data capture applications are used.

(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.

STANDARD CONTRACT CLAUSES

Please refer to the following European Commission website for Standard Contractual Clauses (SCC) between an EU controller to non-EU or EEA controller:

https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en