1.0 PURPOSE

This policy describes the laws, policies and procedures that must be followed to protect the privacy of biospecimen donors for the GTEx program.

2.0 SCOPE

This policy covers all protected information collected about human beings, and all protected information created, used or disclosed during program related or project related activities. It applies to all individuals who conduct or assist with research, or who otherwise use or disclose protected information about human beings in connection with activities through GTEx.

3.0 DEFINITIONS

3.1 Anonymous Data**:** Information that was previously recorded or collected without any private information for which identity is readily ascertainable under the HHS regulations at 45 CFR 46.102(f), or any of the 18 HIPAA identifiers as listed in **List of HIPAA Identifiers, ER-0001-F1**, and no code is assigned which would allow data to be traced to an individual.

3.2 Authorization: Pursuant to HIPAA rules, a customized document, usually as a part of the informed consent document, that gives an Investigator permission to use protected health information (PHI) as specified in HIPAA for a specific purpose, or to disclose PHI to a third party specified by the Investigator other than for treatment, payment or healthcare operations.

3.3 BBRB -The Biorepositories and Biospecimen Research Branch within the Cancer Diagnosis Program, Division of Cancer Treatment and Diagnosis of the National Cancer Institute (NCI).

3.4 Coded Information/Data: Identifying information that has been replaced with a number, letter, and/or symbol, and a key to enable linkage of the replacement number, letter or symbol to the information.

3.5 Covered Entity: A health plan, a health care clearinghouse, or a health care provider who transmits health information and is therefore subject to the HIPAA regulations.

3.6 Data Use Agreement (DUA): An agreement between the provider and the recipient of the PHI as set forth in HIPAA rule. This agreement establishes who is permitted to use or receive a limited data set; and provides that the limited data set recipient will:

- 3.6.1 Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;
- 3.6.2 Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;
- 3.6.3 Report to the covered entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;
- 3.6.4 Ensure that any agents, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and
- 3.6.5 Not identify the information or contact the individuals

3.7 De-Identified Health Information: As set forth in the HIPAA rule, health information that has been stripped of all identifiers, listed in the **List of HIPAA Identifiers, ER-0001-F1**, so that the information could not be traced back to an individual. De-identified data also pertains to health information that has been assigned and retains a code or other means of identification provided that:

- 3.7.1 The code is not derived from or related to the information about the individual;

3.7.2 The code could not be translated to identify the individual; and

3.7.3 The covered entity (as described above) does not use or disclose the code for other purposes or disclose the mechanism for re-identification.

3.8 Designated Record Set: A group of records maintained by an entity that includes medical and billing records about an individual for the purpose of treatment, payment, or provision of health care. Research records that are not contained in the participant's medical record are not likely to be a part of the designated record set.

3.9 ERA: Ethical and Regulatory Affairs is the functional area that oversees the implementation of regulatory compliance related to protected information.

3.10 HIPAA: Health Insurance Portability and Accountability Act. Statutory law that governs the use and disclosure of Protected Health Information.

3.11 Individually Identifiable Health Information: Under HIPAA, any information collected from an individual (including demographics) that is created or received by a health care provider, health plan, employer, and/or health care clearinghouse that relates to the past, present or future physical or mental health or condition of an individual, or the provision of health care to an individual or the past, present or future payment for the provision of health care to an individual and identifies the individual and/or to which there is reasonable basis to believe that the information can be used to identify the individual.

3.12 Study Management Group: A group providing integrated program management, operational, developmental, and analysis support requiring integration of biomedical science and informatics capabilities.

3.13 Limited Data Set (LDS): Under HIPAA, refers to PHI that excludes 16 categories of direct identifiers and may be used or disclosed, for purposes of research, public health, or health care operations, with a data use agreement and without obtaining either an individual's authorization or a waiver or an alteration of Authorization for its use and disclosure.

3.14 Minimum Necessary Standard: The least information reasonably necessary to accomplish the intended purpose of the use, disclosure, or request of PHI under HIPAA.

3.15 OHRP: Office for Human Research Protections.

3.16 Personally Identifiable Information (PII): Under the Privacy Act, PII is any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, SSN, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information that is linked or linkable to an individual.

3.17 Preparatory to Research: Under HIPAA, any action taken in assessing the research question or hypothesis, such as accessing medical records, querying of databases for any type of individually identifiable health information, or any activity where PHI is accessed to prepare a research protocol.

3.18 Private identifiable information: Under HHS human subject protection regulations at 45 CFR 46.102(f), information which individuals can reasonably expect will not be made public (such as a medical record) which is individually identifiable such that the identity of the subject is or may readily be ascertained by a research investigator or associated with the information.

3.19 Protected Health Information (PHI): Individually identifiable health information as defined in the HIPAA regulations (45 C.F.R. § 160.103), that is or has been collected or maintained by the covered entity in the course of providing healthcare that can be linked back to the individual participant.

3.20 Protected Information: Reference used throughout this document to collectively refer to personally identifiable information, private identifiable information, Protected Health Information and program-specific or project-specific information deemed to be sensitive or confidential in nature.

4.0 RESPONSIBILITIES

4.1 **Staff who use, receive, have access to, disclose or are responsible for protected information about human beings** shall:

- 4.1.1 Include all staff who require access to this data to perform their jobs
- 4.1.2 Attend initial training and adhere to this policy. Attend Refresher Training every 3 years from date of initial/subsequent training.
- 4.1.3 Report modifications to the project design that have an impact on the use and disclosure of protected information must be reported promptly to the ERA Team.

4.2 **Ethical and Regulatory Affairs (ERA)** shall:

- 4.2.1 Include members of this functional area within the GTEx program
- 4.2.2 Develop this policy and ensure the adequacy of procedures implemented to protect the privacy and confidentiality of information collected, processed, stored or transferred as part of activities for GTEx.
- 4.2.3 Develop related training materials and monitor the training of pertinent staff regarding protected information.
- 4.2.4 Serve as consultants to all other Functional Areas, project teams and collaborating parties for use and disclosure of protected information collected, processed, stored and transferred to any other parties by the GTEx program.
- 4.2.5 Assess modifications and revise strategy for compliance with HIPAA, 45 CFR Part 46, The Privacy Act, and relevant guidance including but not limited to OHRP's Guidance on Research Involving Coded Private Information or Biological Specimens.

4.3 **Program Directors and Functional Area Leads** shall:

- 4.3.1 Include BBRB and the Study Management Group program directors and functional area leads.
- 4.3.2 Attend training and adhere to this policy.
- 4.3.3 Prior to the start of a project (basic, clinical, pre-clinical, non-research), consult with the ERA team to identify if the project involves the use of or disclosure of protected information. This includes projects or statements of work performed by individuals on behalf of the GTEx program.
- 4.3.4 Report all modifications to the project design that have an impact on the use and disclosure of protected information to the ERA Team.
- 4.3.5 Verify that their assigned staff has taken HIPAA Awareness and Education training prior to involvement with GTEx activities and that Refresher Training is completed every 3 years from date of initial/subsequent training.

5.0 POLICY

5.1 Policy – The GTEx program will protect all *personally identifiable* or *sensitive information*, as defined by the Privacy Act of 1974 (as amended at 5 U.S.C. 552a), *private identifiable information* as defined in U.S. Department of Health and Human Services' (HHS) regulations protecting human research subjects (45 CFR part 46), *protected health information* (PHI), as defined in the HIPAA Privacy Rule (45 CFR 160 and 164), and other information deemed sensitive or confidential according to program or project-specific policies or initiatives. This policy is intended to limit unauthorized or inappropriate use, receipt, storage, and/or disclosure of protected information while at the same time making such information accessible, as appropriate, to necessary parties.

5.2 Compliance with this policy requires compliance with all applicable state and local laws or regulations that provide additional privacy protections for human data.

5.3 The GTEx program will ensure project-specific language, which may state provisions on data protection, is observed as they are considered obligations. As stated above, all applicable local and state laws should be observed.

6.0 REFERENCES

6.1 HIPAA regulations at 45 CFR Parts 160 and 164
http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf

6.2 HHS Human Subject Protection Regulations at 45 CFR Part 46

6.3 The Privacy Act of 1974, as amended at 5 U.S.C. 552a.
http://www.hhs.gov/foia/privacy/index.html

6.4 OHRP Guidance on Research Involving Coded Private Information or Biological Specimens, August 10, 2004. http://www.hhs.gov/ohrp/policy/cdebiol.html