LONG ISLAND UNIVERSITY

COLLECTION, MANAGEMENT, AND SECURITY OF RESEARCH INFORMATION POLICY

PURPOSE

All faculty, staff and/or students conducting research involving human participants are responsible for protecting information associated with research activities and taking appropriate steps to prevent the unauthorized release of individually identifiable research information, in full compliance with applicable Federal and State regulations and University policies. Such information includes, but is not limited to, academic records, medical or health information, Social Security numbers, individually identifiable financial information such as numbered accounts from credit card companies, financial institutions, and related private information.

STATEMENT OF POLICY

Medical records containing protected health information may be subject to additional privacy protections as required under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations and the 2009 HITECH Amendments. Academic records may be protected by provisions of the Family Educational Rights and Privacy Act (FERPA) of 1974. Identifiable personal data collected from individuals located in European Economic Area countries may be protected by the General Data Protection Regulation (GDPR). If research data contains personally identifiable information, sensitive information, or information subject to additional protections such as HIPAA, FERPA, and/or GDPR, it must be securely transmitted and stored at all times. Some federal agencies have additional compliance regulations in order to receive grant awards related to research that must also be met, when applicable.

The Institutional Review Board (IRB) requires that appropriate security measures be taken when the collected data, both electronic and physical documents, are being stored, shared and transmitted. Electronic data refers to any information recorded in such a manner that it requires a computer or other electronic device to display, interpret, and/or process the information. Physical documents refers to any information recorded in such a manner that it can be directly used by an individual without requiring a computer or other electronic device to display, interpret, and/or process the information. The required security measures correlate to the sensitivity and confidentiality of the collected data and are described in further detail below.

PROCEDURES

See *Collection, Management, and Security of Research Information Procedures.*

DEFINITIONS

Level 1 - De-identified information and other non-confidential information

Definition:
Level 1 information includes all de-identified and other non-confidential information. Research information in which all identifiable private information that could be used, directly or indirectly, to identify an individual has been removed or modified is referred to as "de-identified research information." Non-confidential information

includes publicly available information, such as U.S. Census Bureau data or directory information.

Example:
An example of a Level 1 data set would be data obtained from an anonymous survey where limited demographic information may also be collected.

Storage Requirements:
There are no specific University or IRB requirements for the protection of de-identified research information or for other non-confidential research information; however, the IRB may require additional data protection measures, depending on the research and the data being collected. Researchers may additionally want to protect such data for their own reasons (i.e., keeping data private until a paper about the data is published). Level 1 data security includes maintaining normal computer security precautions as recommended by the LIU IT department.

Level 2 - Benign information about individually identifiable persons

Definition:
Level 2 information includes individually identifiable information, disclosure of which would not ordinarily be expected to result in material harm, but it is information which a subject has been promised will not be disclosed by the research investigator. Data protected by FERPA, HIPAA, or GDPR cannot be classified as Level 2 data.

Example:
An example of a Level 2 data set would be data obtained from surveys about participants' over-the-counter pharmaceutical purchases before and after a benign behavioral intervention, where the participants' identities are collected in order to correlate the surveys completed at two time points.

Storage Requirements:
Level 2 data that include personal identifiers but do not contain any sensitive information should be stored on storage devices that have at least password-level protection.

Level 3 - Sensitive information about individually identifiable persons

Definition:
Level 3 information includes individually identifiable information that, if disclosed, could reasonably be expected to be damaging to a person's reputation or to cause embarrassment. Student academic and other information protected by FERPA, HIPAA, or GDPR are generally categorized as Level 3 data; however, the sensitivity of the data involved may require categorization under Level 4.

Example:
An example of a Level 3 data set would be data obtained about participants' weight, blood pressure, and body-mass index screenings, where the participants' identities are collected and linked to the measurements.

Storage Requirements:
Level 3 data should NEVER be stored on personal devices, including personally-owned laptops, cell phones, etc.; instead, Level 3 data should be securely stored on LIU-owned physical storage devices such as external drives, laptop and desktop hard drives. Level 3 HIPAA-protected data that is owned by LIU must be stored on a HIPAA-compliant LIU computer server. LIU researchers who are using HIPAA-, GDPR-, or FERPA-protected data owned by an outside entity are required to follow the storage requirements mandated by the data source owners. If

the outside entity does not provide specific data storage requirements, then the guidance in this policy must be followed.

Level 4 - Very sensitive information about individually identifiable persons

Definition:
Level 4 information includes individually identifiable High Risk Confidential Information (HRCI). HRCI is highly sensitive information which, if disclosed outside the research context at the level of individually identifiable information, could reasonably place the subjects at risk of criminal or civil liability or be damaging to their financial standing, employability, educational advancement, or reputation. Data protected by FERPA, HIPAA, or GDPR may also fall under Level 4.

Example:
Examples of Level 4 data sets may include those that contain individually identifiable information about illegal activities, socially stigmatizing behaviors, or diagnosis of communicable diseases.

Storage Requirements:
Level 4 data should NEVER be stored on personal devices, including personally-owned laptops, cell phones, etc. If the Level 4 data is HIPAA-, GDPR- or FERPA-protected data and owned by LIU, it must be stored on a HIPAA-compliant LIU computer server. Level 4 data owned by LIU that is not protected by HIPAA, GDPR, or FERPA can be saved on encrypted LIU-owned physical storage devices such as external drives, laptop and desktop hard drives, provided adequate physical controls are in place. LIU researchers who are using HIPAA-, GDPR- or FERPA-protected data owned by an outside entity are required to follow the storage requirements mandated by the data source owners. If the outside entity does not provide specific data storage requirements, then the guidance in this policy must be followed.

Questions regarding these requirements should be directed to the IRB Administrator (516-299-3591) or Information Technology at Brooklyn (718-488-3300) or Post (516-299-3300).

POLICY TYPE: ACADEMIC AFFAIRS