<table>
<tr><td colspan="2">Grand Valley State University
Institutional Review Board (IRB)</td></tr>
<tr><td colspan="2">Title: Collection, management and security of research information</td></tr>
<tr><td>Section: 730.</td><td>This policy and procedure supersedes those previously drafted</td></tr>
<tr><td>Approved by HRRC: 12/06/2011
Revised: 10/28/2014
Reviewed: 10/28/2014
Revised by HRRPPC: 03/28/2018
Revised by IRBPPC: 04/23/2019</td><td>Approved by RIO/HRPA: 12/15/2011
Revisions Approved: 10/28/2014
Revision Approved by AIO/RIO: 4/16/2018
Revision Approved by AIO/RIO: 5/23/2019</td></tr>
<tr><td colspan="2">Effective Date: 5/27/2019</td></tr>
<tr><td colspan="2">Related documents:
120: Compliance with Applicable Laws and Regulations
710: Assessing risk to research participants
OP-6: GV Information Technology policies on data security
G-5: Guidance on assessing risk using magnitude of harm in categorizing risk level
G-6: SACRPP guidance on assessing risk
G-8: OHRP and FDA guidance on withdrawal of subjects from research data retention
G-16: Guidance on data management requirements for research data
PC 11.7: Confidentiality, Data & Security Policy</td></tr>
</table>

Policy

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.

Medical records containing protected health information may also 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. See: http://www.gvsu.edu/registrar/ferpa-access-to-student-records-21.htm. 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 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 is described in further detail below.

Guidance

Electronic Data:
Information in electronic formats presents specific challenges to researchers and administrators when planning for methods of collecting, storing, transmitting, controlling access to, and disposing of information that adequately preserves the confidentiality, integrity, and availability of the data. The IRB considers defensive security measures the best course of action to ensure the confidentiality of participant data. Password access when combined with encryption better guarantees that even if the media fall into the wrong hands, the data are less likely to be retrieved. Physical access controls should not be overlooked when planning for adequate security. Physical controls such as locks, when combined with technical controls such as passwords and encryption, provide for a greater depth of defense.

Physical Documents:
Physical documents commonly include paper-based consent forms, data files, medical records, etc. Adequate physical access controls need to be considered, and documents should be securely stored on campus whenever possible. Access to the documents should be restricted to key personnel and supervised by the Principal Investigator of the protocol. Locked file cabinets should be used and preferably located in secured locations (i.e., locked office or laboratory). In the event that research activities are carried out at an off-campus location, and it is necessary to maintain the documents at the research site or another off-campus location, appropriate physical controls must still be used.

Tapes and other media-supporting devices (e.g., flash drives) used for audio and/or video recordings should be stored in the same manner as physical documents and erased as soon as information has been transcribed or coded and is no longer needed for the research.

Transfer of physical documents should be well thought out with particular attention paid to the method of delivery. When paper documents must be transferred, it is recommended that the documents be electronically scanned and sent electronically, if possible; the original paper documents can then remain in a secure location with adequate physical controls.

Identifiable Private Information:
Identifiable private information is defined in the Federal regulations (45 CFR 46.102(e)(5)) as, “private information for which the identity of the subject is or may readily be ascertained by the investigator or associated with the information.” This includes: 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 this linked or linkable to an individual, such as medical, educational, financial, and employment information.

Levels of Protection

Information is categorized into four levels of protection, depending upon the sensitivity and confidentiality of the collected data. The levels of protection identified below are intended as general guidance; the IRB may, at its discretion, categorize data into a higher level and/or require alternative or additional data protections beyond those listed below. The IRB may also conditionally approve a protocol contingent upon final consultation with the GVSU Information Technology (IT) department.

GVSU researchers who are using data owned by an outside entity may be subjected to alternative and/or additional storage requirements by the data source owners. Additional legal restrictions (including, but not limited to, HIPAA or FERPA regulations) may also apply.

Refer to University Policy 11.7: Confidentiality, Data & Security Policy for general information about data confidentiality and security at GVSU. Refer to *G-16: Guidance on Data Management Requirements for Research Data* for additional guidance specific to human subjects research and suggested University resources.

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 GVSU 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 GVSU-owned physical storage devices such as external drives, laptop and desktop hard drives. Level 3 data also may be stored on the GVSU network such as the L: drive with access to the data set restricted to appropriate IT staff and to IRB-approved study team personnel only, via login ID and password. Level 3 HIPAA-protected data that is owned by GVSU must be stored on a HIPAA-compliant GVSU computer server available through the GVSU High Performance Computing Center. GVSU 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 GVSU, it must be stored on a HIPAA-compliant GVSU computer server available through the GVSU High Performance Computing Center. Level 4 data owned by GVSU that is not protected by HIPAA, GDPR, or FERPA can be saved on encrypted GVSU-owned physical storage devices such as external drives, laptop and desktop hard drives, provided adequate physical controls are in place. GVSU 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 ORCI (616-331-3197), the High Performance Computer Manager (616-331-2441), or Information Technology (616-331-2101).