Grand Valley State University Institutional Review Board (IRB)	
G-16: Guidance on data management requirements for research data	
Issued: 09/05/2023 Version: 2.0	Office of Research Compliance & Integrity

Maintaining human subject data securely with the appropriate level of confidentiality or de-identification is a key factor in ensuring a low-risk threshold for the participants, the researchers, and the university. As such, principal investigators and their study teams are required to outline the data management and security procedures in the IRB application. (See *IRB Policy 730: Collection, Management & Security of Research Information* for more information and a classification of data security levels. Each level of security correlates to the sensitivity and confidentiality of the collected data.) Data security levels are verified by the ORCI/IRB during protocol review.

Resources available to GVSU researchers are indicated in the table below. The IRB recommends that research teams consistently follow these recommendations as they correlate to the level of data security being utilized for the project. If you choose to use other resources, you must ensure they meet the required security standards, and documentation of this must be provided in the protocol application. Further information about using external services is provided below.

If your research data contains personally identifiable information, sensitive information, or information subject to additional protections, it must be securely transmitted and securely stored at all times. Common additional protections include the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Family Educational Rights and Privacy Act of 1974 (FERPA), and the General Data Protection Regulation (GDPR). More information about data requirements for HIPAA, FERPA, and GDPR are provided at the end of this document.

To request any of the GVSU IT solutions below, please submit an IT ticket to the appropriate service center.

Level of Security	Data Storage Requirements	Data Transmission/ Transfer Requirements
Level 1: De-identified data and publicly available identifiable information	For Level 1 data, researchers should abide by any College-specific requirements in place. In absence of those, researchers should use one of the following: • GVSU-approved cloud storage available through OneDrive, MS Teams (preferred) or Google. • Shared folder on the GVSU network • Password-protected portable storage device kept in a secure location	It is permissible to download the information from the vendor or client. Options to share the data set with other members of the research team: • GVSU-approved cloud storage available through OneDrive, MS Teams (preferred) or Google. External collaborators can be given access to OneDrive and MS Teams. • Shared folder on the GVSU network. • Password-protected portable storage device in a secure location that is accessible to members of the research team. • Email between GVSU email addresses and/or to non-GVSU email addresses.

Level of Security	Data Storage Requirements	Data Transmission/ Transfer Requirements
Level 2: Benign information about individually identifiable persons **(cannot include FERPA-, GDPR-, or HIPAA-protected data)**	Level 2 data must be protected with at least password-protection. It is recommended that this data be stored on the GVSU network, GVSU-managed MS Teams or OneDrive where access is limited to members of the study team. Use of portable storage devices (i.e. thumb drives, external hard drives) is allowable if they are password protected. Additional encryption is recommended, if available. Level 2 data should not be stored on a personal computer, phone, or cloud-based app longer than needed for the study. If it is necessary to record interviews on a personal phone, computer, or cloud-based app, it is recommended that the recording be moved to a secure location as soon as possible after the interview and then immediately be removed from the personal device/app. The interviews must be removed from the personal device/app at the end of the project if they have not already been removed at an earlier point in the study.	It is permissible to download the information from the vendor or client. Options to share the data set with other members of the research team: • GVSU-approved cloud storage available through OneDrive, MS Teams (preferred) or Google. External collaborators can be given access to OneDrive and MS Teams. Password-protect the file(s) and ensure access is limited to only the research team. • Password-protected shared folder on the GVSU network. • Password-protected portable storage device in a secure location that is accessible to members of the research team. • Email between GVSU email addresses and/or to non-GVSU email addresses.

Level of Security	Data Storage Requirements	Data Transmission/ Transfer Requirements
Level 3: Sensitive information about individually identifiable persons **(includes most FERPA-, GDPR-, and/or HIPAA-protected data)**	Level 3 data must be securely stored via one of the following methods: • GVSU network drive with password protection. If FERPA-, GDPR-, and/or HIPAA-protected data is involved, access control lists must be in place to ensure access is granted only to specific individuals listed by the researchers. • Encrypted portable storage device kept in a secure location. • GVSU-managed MS Teams • Properly vetted cloud-based storage per direction of Academic Research Computing, IRB, and Information Security. Direct identifiers must be removed from the data set and stored in a separate file with a separate password. Use of a Subject ID number is recommended to correlate the identities with the data set. Personal devices (phone, laptop, tablet, etc.) CANNOT be used, even temporarily, to store Level 3 data protected by FERPA, GDPR or HIPAA. Non-FERPA-, GDPR-, and HIPAA-protected Level 3 data can be stored temporarily on personal devices. If using a cloud-based app for recording or transcribing interviews, the app must be vetted and approved by	It is permissible to download the information from the vendor or client. Options to share the data set with other members of the research team: • Password-protected shared folder on the GVSU network. • GVSU-managed MS Teams. External collaborators can be given access to MS Teams. • Keep an encrypted, password-protected portable storage device in a secure location that is accessible to members of the research team. • Mail/hand-deliver the data on a password-protected/encrypted portable storage device. The researcher should call the recipient with the password; do not include it in the mailing or email it separately. • Level 3 data CANNOT be emailed.

	Academic Research Computing prior to IRB approval. This vetting can occur either prior to the submission (by the PI contacting Academic Research Computing and providing documentation of approval in the submission) or during the IRB review process (by the IRB/ORCI initiating the review).	
Level of Security	Data Storage Requirements	Data Transmission/ Transfer Requirements
Level 4: Very sensitive information about individually identifiable persons **(includes some FERPA-, GDPR-, and/or HIPAA-protected data)**	Level 4 data must be securely stored in one of the following areas: • If only a single person will be accessing the data, it should be stored on an encrypted portable storage device. The device must be stored in a secure location. • GVSU network drive with password protection. Access control lists must be in place to ensure access is granted only to specific individuals listed by the researchers. • If more than one person will be accessing the data, BitLocker or REDCap must be used. Contact Academic Research Computing for information. Personal devices (phone, laptop, tablet, etc.) CANNOT be used to store Level 4 data, even temporarily.	When downloading identifiable Level 4 data from a sponsor or collaborator, it is recommended that a secure file transfer protocol is used. Options to share the data with other members of the research team: • Password-protected shared folder on the GVSU network. • BitLocker or REDCap. Each member must have a unique user ID and password to access the data. • Level 4 data CANNOT be emailed.

Passwords versus Encryption

Both passwords and encryption are used to prevent unauthorized access to data. To understand the difference, think of passwords as a padlock and only those who have the key (password) can view the data. Encryption is like scrambling the data before it is protected, and only those who have the encryption code can put the message back together. Encryption is more difficult to break than a password and provides increased protection and security.

To encrypt portable storage devices, follow the directions from the device manufacturer.

Use of External Storage Networks/Services

The resources available through GVSU are supported by IT and meet the necessary security standards for data as outlined above. Collecting or storing research data using external storage networks and services, including internet-based providers, results in additional complexity in ensuring data security standards are met. The jurisdictional authority of the researcher, the location of the study participants, and the location where the data is stored must all be considered. Researchers need to be aware that there may be different data security privacy policies, and in many cases, an agreement between the University and provider may be required. Researchers need to ensure compliance with all laws related to data security, including international laws and export control regulations.

Regardless of data security level, researchers are responsible for ensuring all precautions are met in accordance with all University policies and any respective data use agreements covering the data. Security auditing and data retention/removal agreements are often required when Level 3 or 4 data are involved. Furthermore, cloud-based storage of any Level 3 or Level 4 data must be reviewed by the IT Security team and done through an approved vendor with proper business associate agreement(s) (BAA) in place prior to moving data into the environment. https://www.gvsu.edu/it/storage-off-campus-83.htmhttps://www.gvsu.edu/elearn/help/panopto-68.htm

When utilizing external systems to store and manage data, the "owner" of the data/project should be a faculty or staff member, not a student. This provides for a better continuity of access to the data and better oversight of the destruction of data after the project ends.

Additional Requirements for HIPAA-Protected Data

The HIPAA regulations ensure that personal health information remains protected, and there are significant personal and institutional fines for noncompliance. The HIPAA regulations have additional requirements for data management:

- Identifiable health information should not leave the hospital or institution that owns the data unless a signed legal agreement is in place. For more information on what constitutes identifiable information, refer to the National Institutes of Health's website. It is important to note that dates are considered identifiers.
- HIPAA defines 18 identifiers that constitute protected health information (PHI) that is covered under the regulation:

    - Name
    - Address (all geographic subdivisions smaller than state, including street address, city, county, and zip code)
    - All elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age if over 89)
    - Telephone number
    - Fax number
    - Email address
    - Social security number
    - Medical record number
    - Health plan beneficiary number
    - Account number
    - Certificate or license number
    - Any vehicle or other device serial number
    - Web URL
    - Internet protocol (IP) address
    - Finger or voice print
    - Photographic image – Photographic images are not limited to images of the face.
    - Any other characteristic that could uniquely identify the individual
- If all 18 identifiers have been removed from the data set, the information can be shared outside of the hospital or entity as long as that entity approves of the release. For guidance regarding methods for de-identification of PHI in accordance with HIPAA, refer to the U.S. Department of Health and Human Services' website.
- Identifiable health information should never be stored with cloud storage providers or shared using web-based email. Information stored in these environments may be considered property of the cloud vendor or email provider. This could be considered a breach of confidentiality under the HIPAA regulations. Depending upon the nature of the breach, it may need to be reported to the Office of Civil Rights, the federal agency that oversees HIPAA compliance.
- GVSU offers REDCap as a secure data management option. Access to REDCap can be requested through the service request form. To ensure better continuity of access and destruction after the project ends, the "owner" of the project in REDCap must be a faculty or staff member; students are not allowed to start a project in REDCap.

For more information about HIPAA, contact the GVSU Division of Legal, Compliance & Risk Management (616-331-2067).

Additional Requirements for FERPA-Protected Data

The FERPA regulations protect the privacy of student educational records. FERPA-protected data to be used for research purposes requires written consent from the owner of the data (i.e., the student) prior to accessing the information for the research. FERPA data may not be released to other parties without proper authorization.

FERPA-protected data should never be stored with cloud storage providers or shared using web-based email, unless the researcher has received written confirmation from Academic Research Computing that the provider has been properly vetted and such storage is allowed. Information stored in these environments may be considered property of the cloud vendor or email provider. This could be considered a breach of confidentiality under the FERPA regulations.

For more information about FERPA, please see GVSU IRB Guidance Document *G-17: Guidance on FERPA and Human Subjects Research* and/or contact the GVSU Office of the Registrar (616-331-3327) or GVSU Division of Legal, Compliance & Risk Management (616-331-2067).

Additional Requirements for GDPR-Protected Data

The GDPR protects the privacy and security of personal data collected from individuals in European Economic Area (EEA) countries. All researchers collecting identifiable personal data in, and/or transferring personal data from, EEA countries must operate in compliance with this regulation.

According to the GDPR, a privacy policy and consent form are required when collecting identifiable personal data from someone in an EEA country. The policy states how the data will be used, including when destroyed. The consent allows the individual to give their approval of the data collection and storage plan. If the participant does not grant consent, no identifiable personal data may be collected.

Appropriate technical and organizational measures must be in place to ensure a level of security appropriate to the risk for the collected data. GVSU has secure servers available for researchers who are collecting private identifiable information; researchers are encouraged to use those secure servers for storage of their project data for any project involving personal or sensitive data. Where possible, researchers should also convert identifiable data to de-identified data at the earliest possible point in the project and destroy personal identifying data when possible. (Note: if data destruction is to be a part of the research plan, the participant must be notified of this in the informed consent document.) Using these servers can help ensure data is properly destroyed in the event data removal is requested.

For more information about the GDPR, see Frequently Asked Questions about the GDPR and/or contact the GVSU ORCI (616-331-3197).