Grand Valley State University Institutional Review Board (IRB)	
G-16: Guidance on data management requirements for research data	
Issued: 06/25/2019	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.)

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 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.

Level of Security	Data Storage Requirements	Data Transmission/Transfer Requirements
Level 1: De-identified data and other non-confidential information	Researchers should abide by any College-specific requirements in place. In absence of those, researchers should follow the recommendations listed here.	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: • Use a shared folder on the GVSU network. • Keep a password-protected portable storage device in a secure location that is accessible to members of the research team. • Use GVSU-approved cloud storage available through

		OneDrive, Google Drive, or Blackboard. External collaborators can be given access to OneDrive and Blackboard. • Google Docs may be used, but note that this is not considered a secure site. • De-identified data sets can be emailed between GVSU email addresses and to non-GVSU email addresses.
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 where access is limited to members of the study team. Use of portable storage devices (i.e. thumb drives, external hard drives) is allowable, provided devices are password protected. Additional encryption is recommended, if available. Use of cloud storage is generally not recommended. Level 2 data should not be stored on a personal computer, phone, or cloud-based app. If it is necessary to record interviews on a personal phone, computer, or cloud-based app, the recording must be moved to a secure location as soon as possible after the interview and then immediately be removed from the personal device/app. If using a cloud-based app for recording interviews, ensure the company won't re-use the recordings. Include a copy of the	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. • Keep a 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. • Data can be emailed, provided the file is password protected, Outlook encryption is used when sending the email, and the researcher emailing the data is doing so from a computer with Windows 10. The researcher should call the recipient with the password; do not email it in a separate email.

	vendor’s privacy policy with the IRB application.	
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 **(not permissible if data is protected by FERPA, GDPR, or HIPAA)**. • Encrypted portable storage device. Use of cloud storage is NOT permitted. 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 in order to correlate the identities with the data set. Personal devices (phone, laptop, tablet, etc.) CANNOT be used to store Level 3 data.	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 **(not permissible if data is protected by FERPA, GDPR, or HIPAA)**. • Keep an encrypted 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. • Do NOT use cloud storage services. • Do NOT email identifiable data sets to collaborators. Only de-identified data sets can be emailed to collaborators.
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 **(not permissible if the data is protected by FERPA, GDPR, or HIPAA)**.	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 **(not permissible if data is protected by FERPA, GDPR, or HIPAA)**.

	• If more than one person will be accessing the data, BitLocker or REDCap must be used. Contact the High Performance Computing Manager (616-331-2441) for information. Personal devices (phone, laptop, tablet, etc.) CANNOT be used to store Level 4 data.	• BitLocker or REDCap. Each member must have a unique user ID and password to access the data. • Do NOT use cloud storage services. • Do NOT email identifiable data sets to collaborators. Only de-identified data sets can be emailed to collaborators.

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) are able to 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. Passwords can be easily broken, which is why they are not recommended for securing sensitive or confidential data. Encryption is more difficult to break 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 Level 1 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, including international laws and export control regulations, related to the data security.

Any content that is posted to a cloud storage system is potentially discoverable. The University does not make any claims of being able to protect this content when stored in the cloud. The content is only as secure as the least secure app your account is connected to, and if you've connected to a vulnerable web browser extension that has excessive access to your account, a hacker may not even need to target you. Instead, they can just target the app that has access to your account.

GVSU's Google Drive, OneDrive, and Panopto services are more secure than most cloud-based storage solutions; however, GVSU does not have any control over the storage location (inside/outside of the U.S.) and would not have any oversight/input into a breach situation. Therefore, these services are not recommended for storage of any personal identifiable information. A more secure and account-protected application like a University network drive is recommended for storing and saving personal information.

Blackboard courses/organizations can be created for storing and sharing Level 1 research information. Credentials can also be created for your colleagues outside of the University to allow them access to Blackboard if needed. Contact the GVSU Blackboard Administrator (bbadmin@gvsu.edu) to setup a new course/organization and to request access for external collaborators.

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 non-compliance. 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 this website: privacyruleandresearch.nih.gov/pr_08.asp. 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 this website: https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html

- 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 two HIPAA-compliant data management solutions: REDCap and Stratus. Contact GVSU's High Performance Computing Manager (616-331-2441) for access to these products.

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. 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 of 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. 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).