Research Data Management

STACEY GARDNER

BENJAMIN J. VESPER, PH.D., MBA

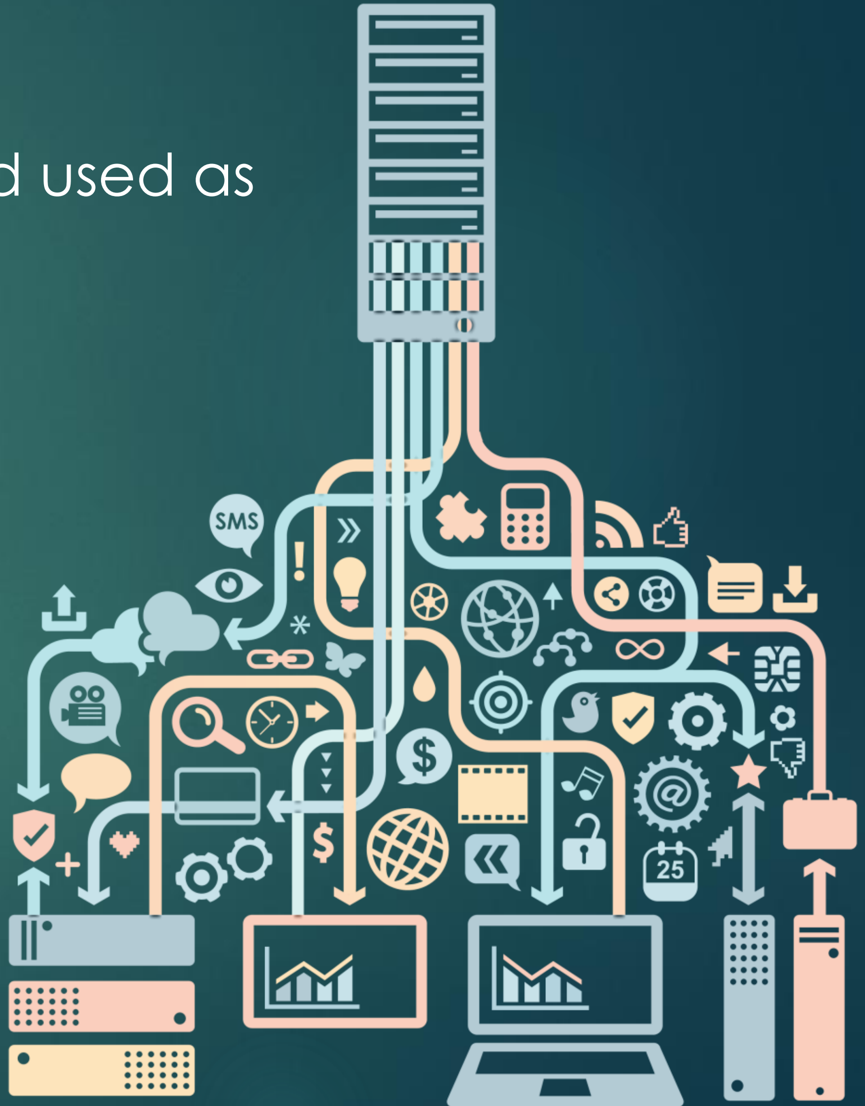
OFFICE OF RESEARCH COMPLIANCE & INTEGRITY

Outline

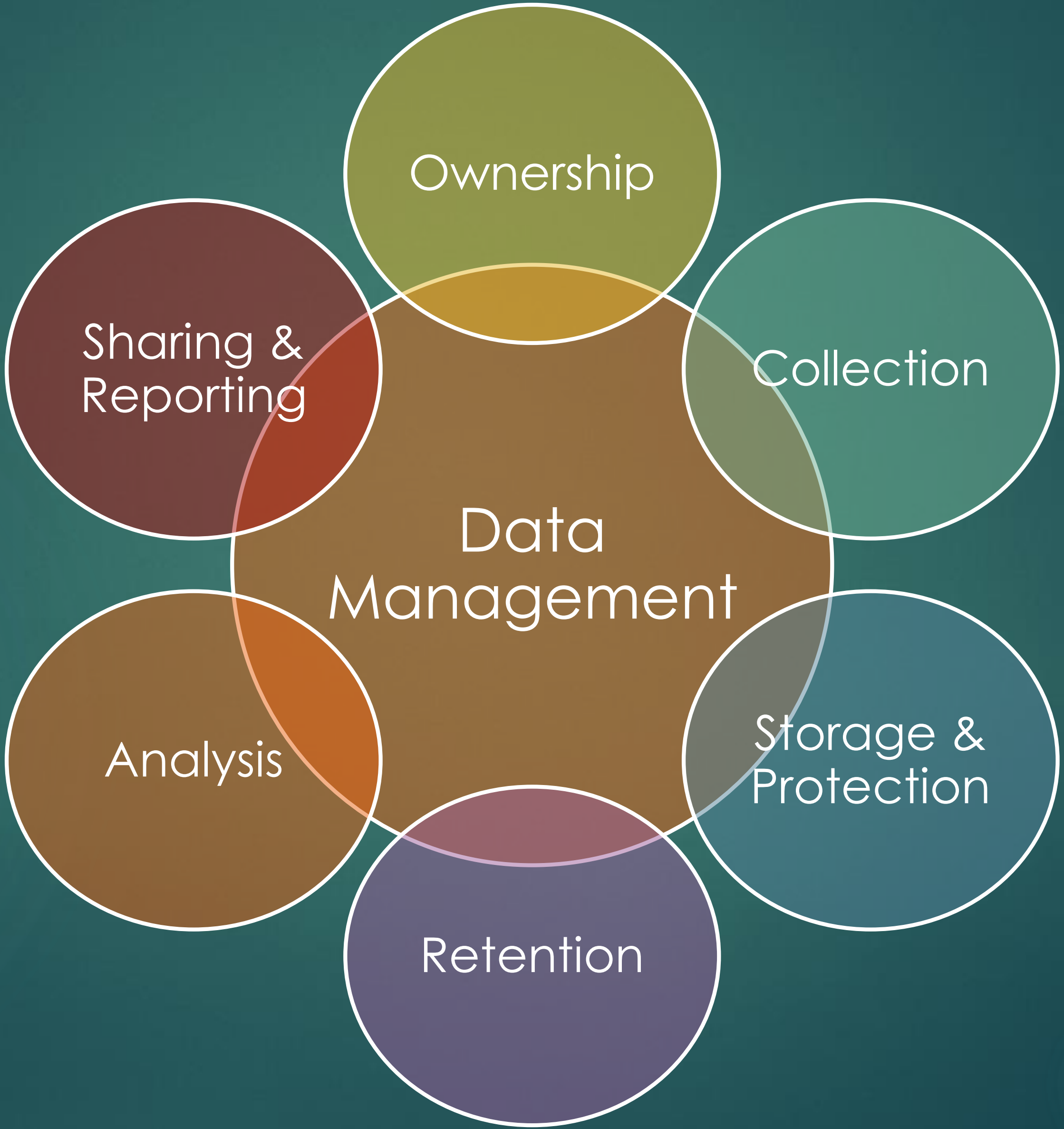
- General information
  - "Guidelines for Responsible Data Management in Scientific Research" funded by the Office of Research Integrity, US Department of Health and Human Services, 2006
- GVSU requirements
- Case studies

What is data?

- Information and observations that are made and used as part of scientific inquiry are considered data
  - Educational tests, surveys & questionnaires
  - Images
  - Audio and video recordings
  - Existing data sets
  - Lab results
  - Biological specimens
  - Investigator observations



Data Management Practices



Data Ownership

The person conducting the research owns the data, correct?

Not always.

- GVSU default is that researcher owns data, but….
- Conditions imposed by funders, collaborating research institutions, and data sources may impact ownership
- Ask these questions _before_ starting your project:
  - Who owns the data I am collecting?
  - What rights do I have to publish the data?
  - Does collecting these data impose any obligations on me?

Data Collection

- Data collection refers to what information is recorded and how it is recorded.
- How does this relate to RCR?
  - Collecting data in a consistent, systematic manner throughout the project (**reliability**) and establishing an ongoing system for evaluating and recording changes to the project protocol (**validity**)

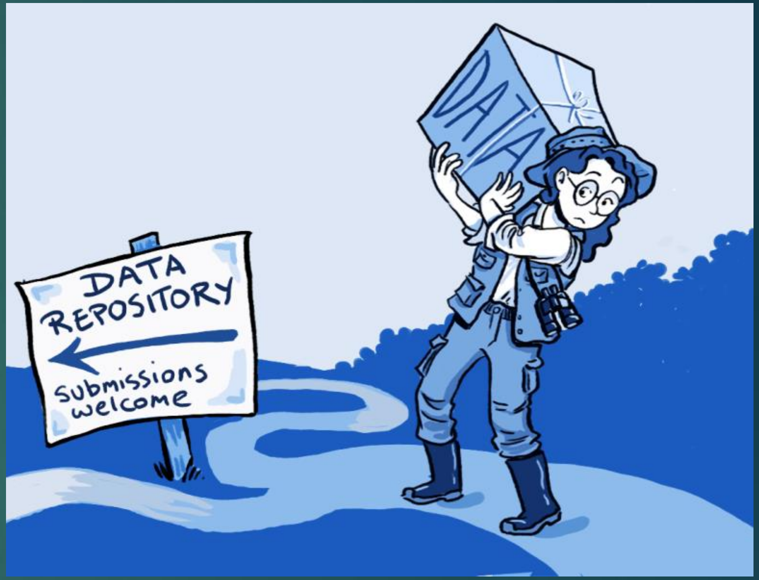
BUT IF WE DIDN'T MEASURE THINGS WE WOULDN'T KNOW HOW GOOD WE WERE AT MEASURING THE THINGS THAT WE'RE MEASURING!
THUMP!
GP

Data Storage & Protection

- Proper storage ensures the data are secure and not subject to corruption.
- Limit who has access to data
- How does this relate to RCR?
  - Concerns the amount of data that should be stored – enough so that project results can be reconstructed
  - Both physical and electronic data need to be protected from physical damage, tampering and theft

Data Sharing & Reporting

- Generally, results are expected to be reported to contribute to the field of study and stimulate new ideas
- Be aware of limitations on dissemination
- Deposit data into public repositories?
- How does this relate to RCR?
    - Concerns how project data is disseminated to others to share important or useful research results; also, when data should not be shared



This Photo by Unknown Author is licensed under CC BY-SA

GVSU Guidance

- IRB Policy 730: "Collection, management and security of research information"
- IRB Guidance Document G-16: "Guidance on Data Management Requirements for Research Data"
- IACUC Handbook of Policies and Procedures, effective 1/1/2020
- Compliance with all University Policies re: data security and computing
- Office of Sponsored Programs Data Ownership Policy currently in development

Data Security Levels

Level 1	**Level 2**	**Level 3**	**Level 4**
De-identified data	Benign identifiable data	Sensitive identifiable data	Very sensitive identifiable data
Cloud storage permitted	GVSU network or encrypted drives	GVSU network or encrypted drives	BitLocker, REDCap, Stratus
No special controls	Email with encryption	HIPAA, FERPA, GDPR	HIPAA, FERPA, GDPR

GVSU Data Sharing & Transfer

Permissible

- Email: Level 1 & 2* only
- Blackboard: Level 1 only
- Encrypted portable storage device
- Mail/hand-deliver
- BitLocker
- REDCap

Not Recommended

- GVSU's OneDrive
- GVSU's Panopto
- Personal devices

Do not use

- Google Drive, iCloud
- DropBox, Box, ShareFile
- Personal devices for any FERPA, HIPAA, GDPR data

* Identifiable level 2 data can be emailed only if encrypted.

GVSU Data Storage

- Cloud storage not recommended for identifiable data, including GVSU’s Google Docs
  - Issues surrounding ownership, discoverability, destruction
- Use of apps for recording and transcription
  - Move to secure location and delete
  - Submit the app’s privacy policy or terms of service for review

Case Studies

Case #1

A professor has developed a novel way to teach a module in her course and wants to determine how well this new method works. She still has hardcopies of past students' assignments and exams, and plans to compare the old assignments and exams with those of her current students. All assignments and exams are in paper form with the students' names on them.

- Is this FERPA-Protected Data?
- Does the professor need to obtain consent from the students to use their assignments/exams?
- What is the best way to store this data?

Case #1: Solutions

- Is this FERPA-Protected Data?
  - Yes
- Does the professor need to obtain consent from the students to use their assignments/exams?
  - Depends. If this work is being done solely to improve the course, no. If this work is being done to generalize the results (i.e., a human subjects research study), yes.
- What is the best way to store this data?
  - Locked file cabinet in locked office

Case #2

A research team wants to conduct an online (Qualtrics) survey about recycling habits. The survey responses will be anonymous, but the researchers will be offering participants a chance to win a $25 gift card as compensation for completing the survey. Those wanting to enter the drawing will be asked to provide their name, home address, phone number, and email address.

- What level of data security would apply to the collected data?
- What are the best storage options for this data?
- What are some best practices the researchers could use to obtain the information needed to distribute the gift card?

Case #2: Solutions

- What level of data security would apply to the collected data?
  - Survey results: Level 1: De-identified data and other non-confidential information
  - Contact information: Level 2: Benign information about individually identifiable data
- What are the best storage options for this data?
  - Password-protected, preferably on the GVSU network.
  - Portable storage device also acceptable (preferably with encryption)
- What are some best practices the researchers could use to obtain the information needed to distribute the gift card?
  - Collect only the information needed. (For example, if sending an electronic gift card, only collect email address. No need to collect name, home address, phone number.)
  - Have a link at the end of the main survey to take the user to a separate survey to collect only the information needed for the gift card drawing. This keeps the study data completely separate from the personal data collected only for the gift card distribution.

Case #3

A GVSU research team wants to work with physicians at local clinics to assess the use and effectiveness of various treatment methods for high cholesterol. The GVSU researchers plan to review patient medical records and interview the clinicians.

Patient medical records: The participating clinics will provide the patient data to GVSU. The data set will include the following: age (not exact birthdate) of the patient, treatment(s) received, dates of treatment, and zip code of residence; all patients will be under the age of 89 and names will not be included in the data set.

Interviews with clinicians: The interviews will be audio recorded using Panopto. The questions will ask about the clinician’s current job title and duties, general characteristics of the patient population served, previous work history as it related to treating cholesterol, and opinions about the use and effectiveness of different treatment methods.

All members of the research team will need access to both the patient medical records and interview recordings.

Case #3: Questions

- Is the patient data HIPAA-protected? Why or why not?
- Who owns the data?
- What level of data security would apply to the collected data?
- What are acceptable ways to store this data?
- The PI of this study has identified a researcher at another university who will help with data analysis of the patient records. He plans to email a password-protected copy of the data file to the collaborator, and will call the collaborator with the password. Is this allowable? Why or why not? If not, how could this data be shared?

Case #3: Solutions

- Is the patient data HIPAA-protected? Why or why not?
  - Yes, due to the inclusion of treatment dates and zip codes.
  - A signed legal agreement would need to be in place with each of the participating clinics.
- Who owns the data?
  - Depends upon the agreement in place between GVSU and the clinics.
  - Most likely: the clinics would own the patient records, and the GVSU researchers would own the data collected from the interviews.
- What level of data security would apply to this data?
  - Interviews: Level 2: Benign information about individually identifiable data
  - Patient data: Level 3: Sensitive information about individually identifiable persons

Case #3: Solutions (Continued)

- What are acceptable ways to store this data?
  - Interviews:
    - Best to use tape recorder if possible
    - If not possible, remove recordings from Panopto as soon as possible after the interview.
    - Store interviews on password-protected network folder limited to members of the study team or password-protected/encrypted portable storage device.
  - Patient data:
    - Portable storage device with password-protection/encryption, or in RedCap or BitLocker.
    - Cannot be stored on GVSU network drive, personal devices, or cloud storage provider.

Case #3: Solutions (Continued)

- The PI of this study has identified a researcher at another university who will help with data analysis of the patient records. He plans to email a password-protected copy of the data file to the collaborator, and will call the collaborator with the password. Is this allowable? Why or why not? If not, how could this data be shared?
  - No, Level 3 data cannot be emailed.
  - Because this is HIPAA-protected data, the agreement with the clinics would need to specify that the data can be released to a third party and under what conditions that data release can occur.
  - Assuming the clinics allow for such data sharing in the agreements: PI could email data after properly de-identifying it or could mail identifiable data on a password-protected storage device and call with the password.

Questions?

Office of Research Compliance and Integrity

- JHZ 049
- Phone: 616-331-3197
- Email: rci@gvsu.edu