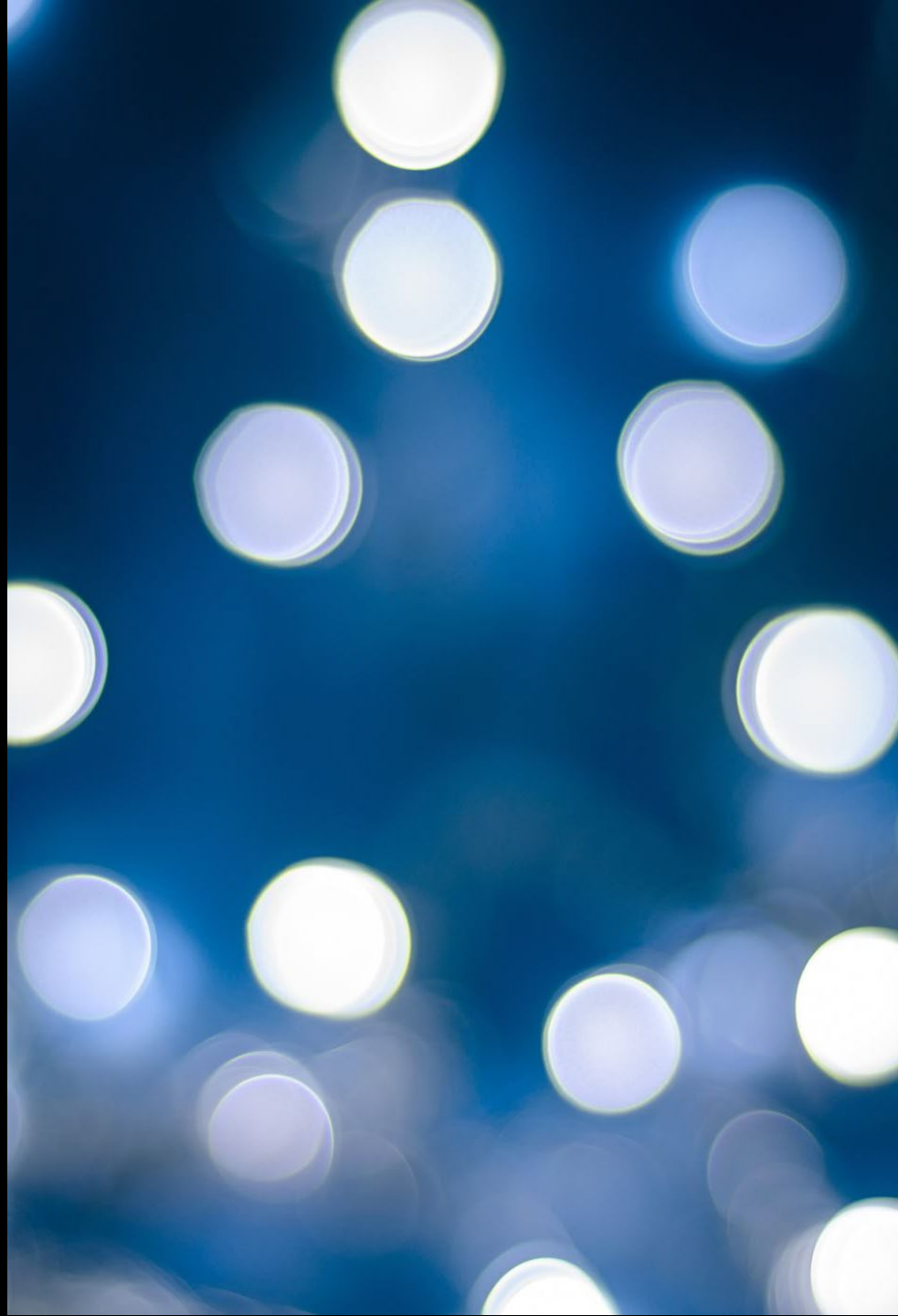
Research Compliance and the role of the Privacy Office

Privacy Office and Human Research Protections Office

Carilion Clinic 2022

Learning objectives

Recognize	The role of compliance and privacy in the review of a research study
Identify	Data security policies for research best practices
Discuss	Responsibilities when there is a data breach.



Poll

In a 2016 study by Black Book, what percentage of U.S. patients state that they withheld some medical information from their providers due to privacy/security concerns?

- 8%
- 32%
- 54%
- 89%

Data breaches impact millions!

From 2005-2019 249 million people were impacted by healthcare data breaches.

157 million people impacted in the last 5 years alone.

Between 2005 & 2019 around 43% of health data was compromised. With hacking incidents exposing more than 92% of EHR records.

The healthcare industry has faced the highest number of breaches among all industries.

Hacking/IT incidents are the most prevalent forms of attack behind healthcare data breaches followed by unauthorized internal disclosures.

Data from the healthcare industry is regarded as highly valuable.

While data hacking is up, unauthorized internal disclosure, theft/loss, and improper disposal of data has decreased.

Main locations for breached healthcare data are email and network servers.

(Seh, 2019)

Poll

What was the estimated cost to healthcare organizations in 2020 due to ransomware attacks?

- $12 million
- $25 million
- $5 billion
- $13 billion

Research data breach Example: 2021

- Survey study exploring breast cancer reconstruction among African American women, offering a $20 Amazon gift certificate for completion.
- Enrollment was slow. After 30 responses enrollment increased notably with 80 completed in 2 days.
- Surveys started coming in in batches that arrived at 2-minute intervals.
- The survey link was open and anyone with it could complete the survey. As the survey was shared it likely attracted bots because of the $20 payment, which was delivered electronically.
- The PI shut the survey down and had to check every survey for things that did not look right such as incomplete surveys, or a response that the individual made $500,000 a year and had Medicaid.
- (Young, 2021)

Research data breach example 2007

- A multi-year medical research study for the Carolina Mammography Registry had the social security numbers of 114,000 women exposed and 180,000 records with names, dates of birth, addresses, phone numbers, demographic information, insurance status, and health history info.
- The breach was not reported to participants until 2009.
- The PI of the study was demoted from a full professor to associate professor and their salary was reduced by nearly half.

Poll

What percent of data breaches involve a human element?

- 10%
- 50%
- 80%
- 100%

- Verizon's 2022 Data Breaches Investigation Report
- 82% of data breaches involved a human element including incidents in which employees expose information directly or by making a mistake that enables cyber criminals to access the organization's systems (Irwin, 2022).

Things to know

- **Privacy: Concerns people**. It is an individual's **right** to be left alone and to limit access to their health care information.
- **Confidentiality: Concerns data.** It is the researcher's **agreement** with the participant about how the participant's identifiable information will be handled, managed, and disseminated.
- **Security:** the systems in place to protect health information.
- **Privacy rule:** protects all individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral (HHS.gov, 2022).
- **Data breach:** an impermissible use or disclosure under the privacy rule that compromises the security or privacy of the protected health information (HHS.gov, 2013).

What is Personal Health Information (PHI)

- Information about a participant's past, present, or future physical or mental condition.
- The provision of their healthcare or payment of it, and
- It somehow reasonably identifies the patient (this can change Big Data, AI, Genomics).
- HIPAA defines data breach as the procurement, access, use or exposure of confidential health information illegitimately, which compromises the privacy or security of that confidential health information.
- 18 identifiers

- Also known as the privacy rule: includes standards and regulations that protect patients from inappropriate disclosures of their protected health information (PHI) that could harm their insurability, employability, and/or privacy.
- HIPAA is the minimum requirement. There may be state or local laws that are more stringent than HIPAA and they MUST be followed.
- HIPAA allows for researchers to access and use PHI when necessary to conduct research.
- Not all research is subject to HIPAA regulations only that which uses or creates PHI.
- Studies using PHI for research MUST have HIPAA in the consent or must request a HIPAA waiver or a partial waiver (for recruitment purposes).
- Institutions are required to establish a “Privacy Board.” The IRBs at Carilion serve as the privacy board:
  - Review and approve requests for waivers of authorization.
  - Disclosures of PHI for research purposes.

Researcher access to PHI at Carilion

- Access to Carilion Clinic's confidential information, including PHI, is a privilege, not a right.
- Human Subjects Research must be approved by the IRB.
- If investigators want to obtain information preparatory to research, they must contact HART for a data extraction or to obtain deidentified data from TriNetX. Please contact the IRB to determine if a Preparatory to Research application is necessary.
- The IRB reviews QA/QI activities to determine if a project is or may be human subjects research. Please submit QA/QI projects for formal approval from the IRB.
- You can request a partial waiver of HIPAA authorization to obtain patient information for recruitment purposes. That request is vetted through the IRB.
- Carilion Clinic Operating Procedure statement on medical research:
    - Conducting medical research is an important part of Carilion Clinic's mission. Federal regulations permit use of your health information in medical research, either with your authorization or when the research study is reviewed and approved by an Institutional Review Board before the study begins. In some situations, limited information may be used before approval of the study to allow a researcher to determine whether eno patients exist to make a study scientifically valid.

We must Safeguard PHI when conducting research

- Follow the rule of “minimum necessary.”
- Only allow approved personnel to have access to PHI.
- Only use approved data storage methods.
- Only use approved data analysis methods.

Noncompliance can result in consequences for Carilion and for Researchers

- Reputation risk
- Disciplinary action
- Epic access blocked
- Regulatory enforcement
- Sanctions
- Licensing Board Action against those involved
- Maximum Annual HIPAA financial Penalties per incident/per patient
  - Lack of knowledge $30,487 per year
  - Reasonable cause up to $121,946 per year
  - Willful neglect timely corrected (within 30 days) $304,865 per year
  - Willful neglect not corrected in 30 days $1.9 million per year
- Civil Action-personally sued
- Criminal penalties- up to 10 years imprisonment

Carilion Human Research Protections Office

The IRB!

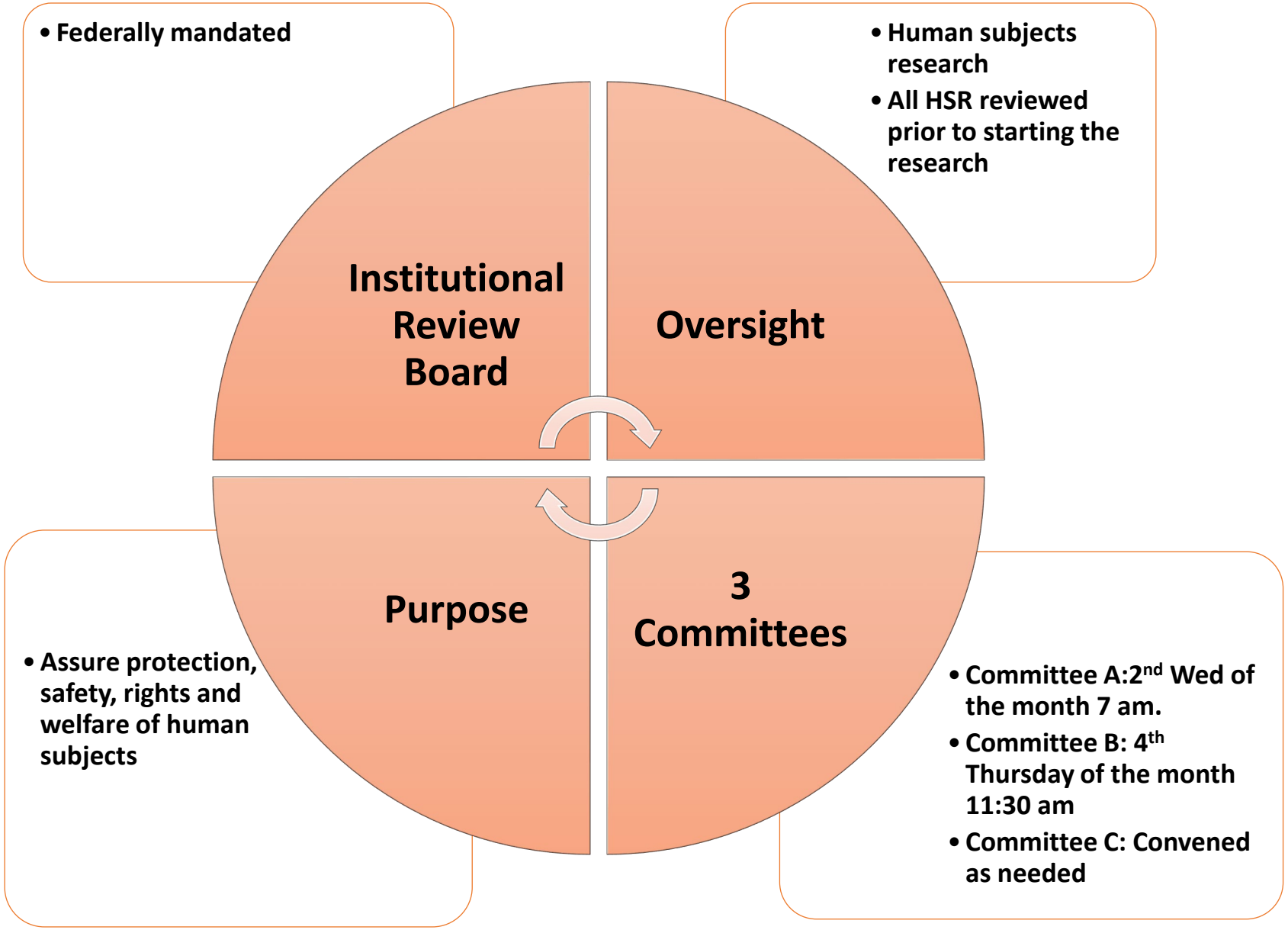
Human Research Protections Office (HRPO) Staff

- Meredith Talmadge (Studies for convened IRB review and Request to Rely submissions) mttalmadge@carilionclinic.org, 540-224-5878
- Brooke Blevins (Minimal risk studies and Not Human Subjects Research determinations) bblevins@carilionclinic.org, 540-224-5882
- Trish Winter (Human subjects research and ethics education manager) pjwinter@carilionclinic.org 540-521-5890
- Tanner Harmon (Staff updates, Closures, Admin Support) Tharmon@carilionclinic.org, 540-224-5883

Responsibilities of the HRPO

- Complies with all local, State, and Federal research guidelines in order to protect human subjects.
- Review and approve exempt and expedited studies
- Quality assurance/quality improvement: Conducts for cause and random on-site reviews and assists with quality improvement activities.
- Education and Outreach: Provides education and training for Carilion researchers, student researchers and IRB board members.
- IRB Review: Carilion has 3 federally mandated Human Research Review Committees (HRRCs) that are responsible for:
  - Reviewing and approving all Full-Board studies
  - Reviewing and managing reportable events.
- Collaboration across the organization:
  - Research and development
  - Compliance
  - Legal Counsel
  - Health Analytics Research Team (HART)

Functions of the IRB



IRB Authority

Risk Determination

Levels of IRB Review

Not Human Subjects Research (NHSR)

Full Board

- More than "minimal risk" to subjects
- Not covered under other review categories
- Example: interventions involving physical or emotional discomfort or sensitive data

Expedited

- Not greater than minimal risk
- Fits one of the 9 Expedited Review Categories*
- Examples: Collection of biospecimens by noninvasive means, Research with existing documents/record collected for non-research purposes in which subjects are identifiable

Exempt

- Less than "minimal risk"
- Fits one of the 8 Exempt Categories*
- Example: Research with de-identified records, anonymous surveys

Threats to data protection

Threats to privacy

- Data collection without the explicit and informed consent of the participant.
- Breaches where collected data becomes accessible to people not identified at the time of collection.
- Collected data must be used according to the specific purposes identified in the recruitment material.
- Specific threats include:
  - access for colleagues in the same cloud environment,
  - human error revealing private information,
  - glitches in connectivity,
  - external hacks.

Threats to confidentiality

- Re-identification of participants,
- Economic incentives for hackers,
- Readily available personal information about large numbers of people .

Minimizing research data security threats

- Handle only the minimum amount of sensitive data strictly needed for the research study.
- Separate Protected Health Information (PHI) from all other data as soon as possible.
    - Once separated, store identifiers separately, analyze data separately, and transmit separately.
- Identifiers should remain encrypted at all times and identifiers and research data should only meet again if necessary to adjust the data matching technique.
- Use encryption capable storage options: SPARC, RedCap, Carilion secure server, Carilion secure email (state this in the IRB application).
- Avoid transmission of identifiable data. If you must send identifiable data make sure that the file is encrypted.
- Train all research partners on handling or transmitting data, data collection procedures, storage, and transfer policies. Request all partners notify the research team before sharing any data to ensure compliance with the data protocol.
- Reference study ID numbers rather than PHI. Develop standard operating procedures for checking in and responding to breaches.
- A standard operating procedure should include
    - Process for sharing data and receiving updates,
    - Process for verifying data set does not contain unauthorized information prior to downloading if possible,
    - Timeline for reviewing new data for unauthorized PII,
    - Plan for notifying the source of the breach and requesting corrective action to further breaches,
    - How files with unauthorized information will be removed and destroyed.

(O'Toole, et al., 2018)

Data security best practices for researchers

- Know what type of data your research is generating, where it is located and have an accurate inventory of it.
- Know how data will be transmitted and what methods are in place to keep that data secure.
- Know how data will be stored, on a portable device or removable media. If so, where will that be stored and used?
- Know if research data is being backed up. If so, by whom, to what location, and how often? How are backup copies secured and are the copies encrypted?

Secure Data Sharing with Researchers & Collaborative Institutions: Carilion Policy

- We do have Memorandums of understanding with Virginia-Tech, Radford, and Virginia College of Medicine.
- SPARC provides Carilion researchers and collaborative researchers with a central location for access to and processing of PHI, limited data sets, and de-identified data for research and grants. Can also be used for Carilion QA/QI projects.
- All research applications that involve collaborations with external institutions, and for which an external institutions IRB will serve as the IRB of record, must be submitted through the PRIS3M system as a request to rely application.

Navigating the IRB Application
Getting Started

- Obtain R&D approval prior to submission of the IRB application.
- Make sure your conflict-of-interest training and annual COI disclosure are filed through Carilion's Office of Organizational Integrity.
- List who is on the study team and their roles and responsibilities. Per Carilion policy the PI is ultimately responsible for all study activities.
- List funding from outside sources for potential conflicts of interest.
- FDA and NIH studies have special considerations be aware when you are completing the application.
- Indicate if there are outside collaborators on the project. If so whom, and are there members of the study team that are under the jurisdiction of another IRB (Virginia Tech students, Radford students, Virginia Tech employees, Radford Carilion employees, etc.)?
- Indicate if Carilion will serve as the IRB of record or if the study team is seeking a request to rely on another IRB.

Study communication and oversight

- How will you manage the communication of information to other sites and back to the Carilion IRB, such as reporting of unexpected problems, protocol modifications, and interim results?
- What is the Carilion Clinic's investigator plan for oversight of research activities at other sites including verification of institutional approvals, data safety monitoring, and ensuring data quality and integrity?
- Will identifiable data or specimens be transferred, transmitted, or shared outside of Carilion? For example, transfer of data or specimens from Carilion Clinic to an external collaborators.
- What types of specimens and/or data, including specific datapoints, will be shared?
- What are the methods of storage of the data at the collaborating site?
- What is the process for shipping specimens and/or transmitting data to the collaborator, including the method of encryption if sharing data electronically?

List of PHI

(Protected Health Information)

- Names
- Dates
- Addresses / Zip Codes / Geocodes
- Phone Numbers
- Fax Numbers
- Email Addresses
- Social Security Numbers
- Medical Record Numbers
- Health Plan Beneficiary Numbers
- Account Numbers
- Certificate /License Numbers
- Device Identifiers
- Vehicle Identifiers
- URLs
- IP Addresses
- Biometric Identifiers
- Facial Images
- Any Other Unique Identifiers

IRI
Total Data Management

- City, town, state, or full zip code;
- Dates such as admission, discharge, service, DOB (under age 89), DOD;
- Ages in years, months, days, or hours.

Deidentifying PHI: Carilion Policy

- PHI that is fully de-identified in accordance with HIPAA may be accessed, used, and disclosed without patient authorization using the following 2 methods:
    1. Using the Safe Harbor method requires removal of all 18 HIPAA identifiers of the individual, or of relatives, employers, or household members of the individual, to be removed in their entirety prior to the access, use, and disclosure of information.
    2. Deidentification by expert determination conducted by HART. Determines that the risk is very small, and that the information could be used alone or in combination with other reasonably available information that identify the individual and that these findings are documented.

Poll

You want to use a limited data set for your online survey study with 30–50-year-old adults with asthma. Which of the following is a LDS?

- Only collecting the patient's health plan beneficiary number and their zip code.
- Only collecting the IP addresses from respondents.
- Only collecting their birth year and full zip code.
- Only collecting their name and medical record number.

Consent: Data collection and data storage

- Will you be obtaining written consent?
- Will you be requesting a waiver of written consent? Do you know the requirements for a waiver of written consent?
- If you obtain written consent be sure to use the Carilion template which includes language for a HIPAA authorization for potential participants.
- Will you request a full or partial HIPAA waiver?

Privacy and confidentiality

- What data points will be reviewed, collected, recorded or created for research purposes including screening or recruitment?
- Is any of the data being collected from the medical record?
- Is the requested private information the minimum necessary to meet the research goals?
- Will the research records (other than the consent form) and/or specimens contain data that is identifiable, coded, or de-identified?
- Attach a data collection sheet or clearly list ALL of the data collection points for your study.

- How will the research data will be stored and managed?
- How long will research records, data, and specimens be retained following **completion of the study**? Where will study records will be retained when the study has been closed (long-term storage)?

Describe when and how the identifiers, if applicable, will be destroyed. If specimens will be retained, describe where.

Please note that any data involving PHI must be maintained for a minimum of 6 years, and data that does not contain PHI must be maintained for a minimum of 3 years. In many cases, identifiers will need to be retained after the research is completed (e.g., for publication or data verification purposes or because of contractual requirements or grant terms).

Describe the structure of the code (e.g., randomly generated number, sequential number plus initials, etc.) and indicate whether a linking file (key) will be created and, if so, how it will be protected.

Who will have access to identifiers?

How will access to identifiers be protected?

Will research records include information that subjects or others might consider to be sensitive in nature? Explain what sensitive information is included, why it is needed, and any additional safeguards that will be taken to protect it.

- If you are using audio or video recording you will answer additional questions about that data.

Recruitment, risks, and data safety monitoring

- How will subjects be contacted, who will contact them and how will they be introduced to the research?
- Will you need a partial HIPAA waiver in order to find participants appropriate for the study?
- Will pre-screening information be retained on persons who do not ultimately participate in the study and what specific information, including identifiers, will be retained?
- List the possible risks, discomforts, or harms to subjects associated with the research: Be sure to include loss of confidentiality and describe how the research team will minimize this risk.
- Describe the data safety monitoring plan: Include:
  - The data that will be reviewed, including safety data, untoward events, and efficacy data;
  - Who is responsible for reviewing the data;
  - How the safety information will be obtained and documented (e.g., case report forms, by telephone calls with participants, printouts of laboratory results, etc.);
  - The frequency or periodicity of review of cumulative data;
  - The statistical tests for analyzing the safety data to determine whether harm is occurring;
  - Any conditions that trigger an immediate suspension of the research or other action for the research

Data Safety Monitoring Plan (DSMP)

Ensuring the safety of research participants

Purpose

ENSURE THE SAFETY OF RESEARCH PARTICIPANTS

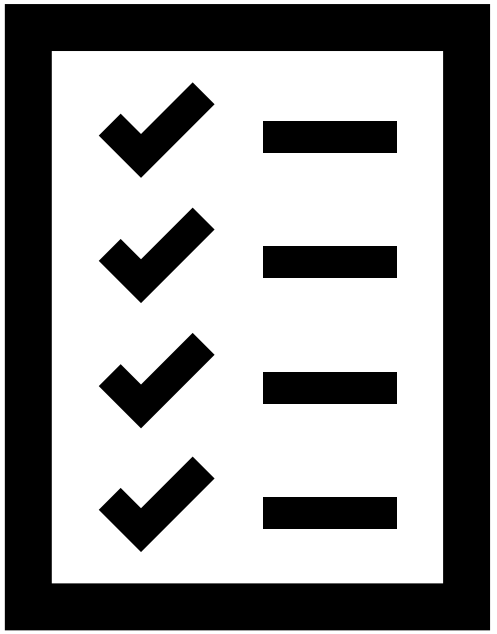
PROTECT THE VALIDITY OF THE DATA

PROTECT THE INTEGRITY OF THE STUDY

ASSURE QUALITY OF THE RESEARCH STUDY

Why should you create a DSMP?

- 45 CFR § 46.111: For IRB approval the following must be addressed:
  - (1)(2)Risks to subjects are minimized and are reasonable in relation to anticipated benefits
  - (6)The research plan makes adequate provisions for monitoring the data collected to ensure safety of subjects
  - (7) when appropriate there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data



Who provides the appropriate level of monitoring for the DSMP?

THE PRIMARY INVESTIGATOR WILL MONITOR (MINIMUM REQUIREMENT)

AN INTERNAL DATA SAFETY MONITORING BOARD WILL BE CONVENED TO MONITOR

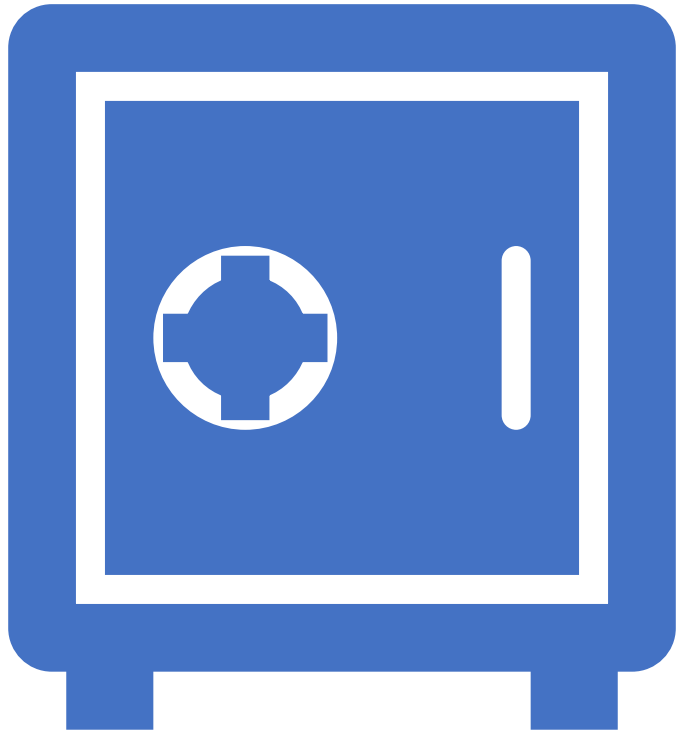
AN EXTERNAL INDEPENDENT BOARD WILL BE CONVENED TO MONITOR

Examples of monitoring activities to ensure subject privacy

- Under what conditions will a subject be screened, recruited, consented, interviewed, and/or contacted?
  - Who will observe the consenting process, interview process, or clinical visits? How often will these observations take place?
  - Where will the consent process occur? Make sure it is in private location.

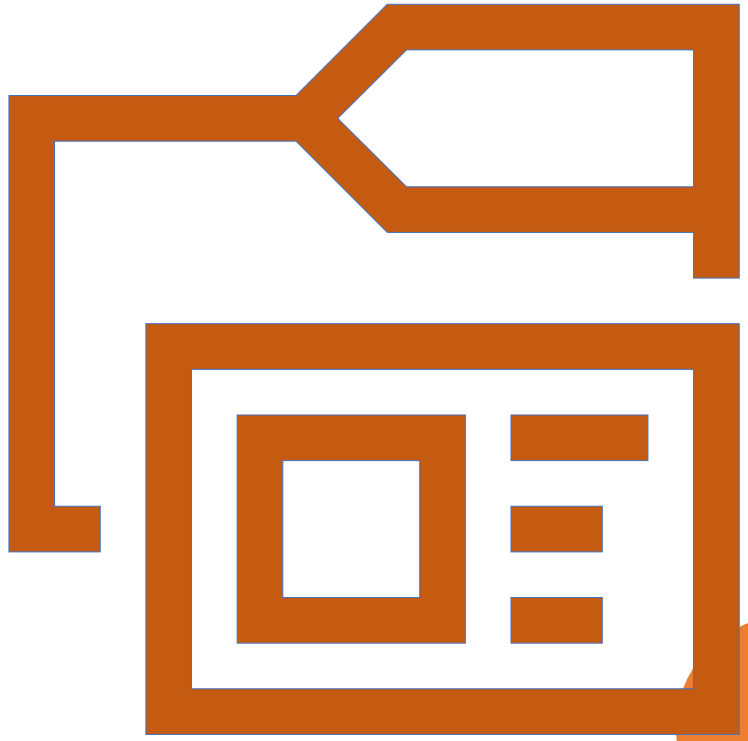
Data Confidentiality

- What are the conditions that will protect the confidentiality of the data?
  - Is information stored in locked filing cabinets, how are electronic records secured, where is PHI stored, how is data being transferred between partner sites, and among multiple sites?



Study documentation

- Who manages study files
- Are there checklists and/or guidelines for monitoring documentation?
- Will the PI sample study files quarterly, annually, after a certain number of participants have completed the trial?



Additional things to consider

The Carilion IRB application includes a data safety monitoring section. This is not optional. All full-board studies require the PI to outline a plan for data safety monitoring.

The IRB team needs to understand how patient safety will be monitored, how data safety will be assured, whether the study is viable, and how data will be handled such as statistical analysis procedures and who will have access to both identified and deidentified data.

If you have questions, contact the IRB to discuss the DSMP

Important considerations for publications

- Articles, papers or other products of research shall not divulge patient identity without authorization of the patient or legal representative.
- All research involving human subjects including research based solely on health records shall be submitted to and approved by the IRB.
- Carilion requires and monitors the appropriateness of access to, or the use and disclosure of PHI created or used for research through the IRB office, Office of sponsored projects, Health Information Management, Clinical effectiveness, the Privacy Office, and others.
- If you have completed a quality improvement/quality assurance project, as identified by the IRB you need to acknowledge that the project is NOT human subjects research.
- Privacy Office: Obtain authorization for case study presentations/publications.

References:

- HIPPA Journal (2022, Jan 23rd). What are the penalties for HIPAA violations. Retrieved from: https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/
- Irwin, L. (2022, July 1st). Human error is responsible for 82% of data breaches. *GRC eLearning*. Retrieved from: https://www.grcelearning.com/blog/human-error-is-responsible-for-85-of-data-breaches#:~:text=According%20to%20Verizon's%202022%20Data,to%20access%20the%20organisation's%20systems.
- Jamieson, T., Salinas, G. (2018). Protecting human subjects in the digital age: issues and best practices of data collection. *Survey Practice, 11*(2). Retrieved from: https://www.surveypractice.org/article/4405-protecting-human-subjects-in-the-digital-age-issues-and-best-practices-of-data-protection
- Manning, B., Perry, R., McKell, A. (2020, Nov.). Research best practices: Privacy, information, risk management, and compliance. *Office of Continuing Development Education Research Series.* Retrieved from: https://www.carilionclinic.org/research11-19-20
- Muchmore, S. (2022, July 28th). Healthcare remains costliest industry for data breaches. *Healthcare Dive. Retrieved from: https://www.healthcaredive.com/news/healthcare-breach-costs/628344/#:~:text=The%20cost%20of%20the%20average,by%20pharmaceuticals%20at%20%245%20million.*
- O'Toole, E., Feeney, L., Heard, K., Naimpally, R. (2018). Data security procedures for researchers. *Abdul Latif Jameel Poverty Action Lab North America: Massachusetts Institute of Technology.* Retrieved from: https://www.povertyactionlab.org/sites/default/files/data-security-procedures.pdf
- Schaffhauser, D. (2009, Oct.10th). U North Carolina undertakes review in face of 7-state data breach. *Campus Technology.* Retrieved from: https://campustechnology.com/articles/2009/10/09/u-north-carolina-undertakes-review-in-face-of-7-state-data-breach.aspx?m=1
- Seh, A.H., Zarour, M., Alenezi, M., Sarkar, A.K., Agrawal, A., Kumar, R., Khan, R.A.(2020). Healthcare data breaches: insights and implications. *Healthcare, 8*(2), 133. Retrieved from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/
- Wager, K.A., Lee, F.W., & Glaser, J.P. (2017). *Health care information systems: A practical approach for health care management (4th ed.),* Jossey-Bass.
- Young, M. (2021, April 1st). IRBs, Researchers starting to recognize security breaches of online research data. *RELIAS MEDIA*. Retrieved from: https://www.reliasmedia.com/articles/147829-irbs-researchers-starting-to-recognize-security-breaches-of-online-survey-data