Balancing Privacy & Collaboration

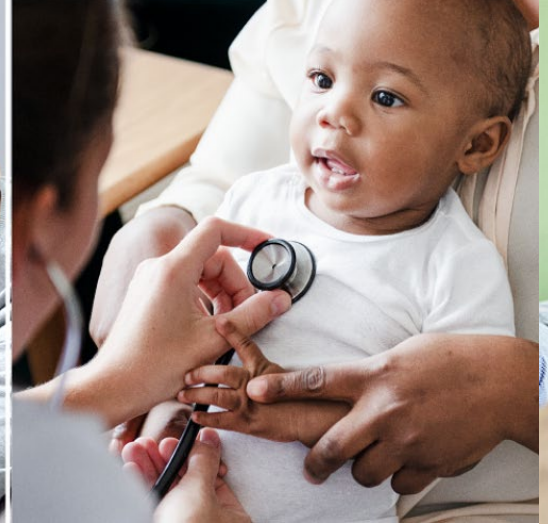
Julie Cook, Director, Privacy and Research Data Protection Program, Scholarly Integrity & Research Compliance, *Virginia Tech*

Katie Tomlinson, Research Compliance Specialist, *Carilion Clinic Privacy Office*

Hilary Hedrick, M.Ed., Human Subjects Research Ethics and Education Manager, *Carilion Clinic Human Research Protections Office & Institutional Review Board*

VIRGINIA TECH

CARILION CLINIC


People.


VIRGINIA TECH

CARILION CLINIC

Our Principles

Mission:

Improve the health of the communities we serve.

Vision:

We provide world-class health care through integrated clinical practice, education and patient-centered research. We develop and respect an experienced, talented workforce. We serve for the love of health.

Values:

COLLABORATION

COMMITMENT

COMPASSION

COURAGE

CURIOSITY

How does your research align with Carilion's mission?

Carilion's Mission

Improve the health of the communities we serve.

Begin the collaboration process with a clear understanding of how the research aligns with Carilion's mission and vision of better patient care, better community health and lower cost.

Terminology

- **Privacy:** It is an individual's right to be left alone and to limit access to their health care information.
  - **Represents people.**
- **Confidentiality:** It is the researcher's agreement with the participant about how the participant's identifiable information will be handled, managed, and disseminated.
  - **Represents data.**
- **Data breach:** The unauthorized use, access, acquisition, or disclosure protected health information (PHI) that compromises the security or privacy of the PHI (OCR, 2013).

HIPAA Privacy and Security Rule

- **Privacy Rule:** Minimum federal standards and regulations that protect patients from inappropriate access, use and disclosures of their protected health information (PHI).
  - Applies to **health plans, health care clearing houses, and health providers (covered entities)**.
  - Requires appropriate safeguards to protect privacy of PHI.
  - Sets limits and conditions on the uses and disclosures that can be made.
  - Gives patients' rights over their PHI.

Applies to all formats of PHI including paper, electronic and verbal

HIPAA Privacy and Security Rule

- **Security Rule:** Establishes a national set of security standards for protecting electronic PHI and operationalizes the protections contained in the Privacy Rule by addressing technical and non-technical safeguards that covered entities must put into place.
  - **Administrative safeguards**: security management process, security personnel, information access management, training, and evaluations
  - **Physical safeguards:** facility access control, workstation and device security
  - **Technical safeguards:** access control, audit controls, integrity controls and transmission security

Privacy Board

- Institutions are required to establish a “Privacy Board”
- The Institutional Review Board (IRB) at Carilion serve as the privacy board:
  - Review and approve requests for waivers of authorization
  - Disclosures of PHI for research purposes

Who must comply with the HIPAA Privacy Rule?

Virginia Tech is not a covered entity

- Data collected by Virginia Tech researchers are not regulated by HIPAA but are regulated by federal and state laws
- Virginia Tech has entered into Business Associate Agreements in a few instances
  - Conducting Virginia Tech research is rarely considered ‘performing tasks on the behalf of a covered entity’
  - This is not a recommended path for research

Who must comply with the HIPAA Privacy Rule?

- Business Associates of a covered entity
  - Performs tasks on behalf of a covered entity that involve access to identifiable health information
    - Quality assurance reviews
    - Billing and claims processing
    - Companies like Zoom may enter into a Business Associate Agreement with covered entities

Role Based Access Control Model

- Access to PHI at Carilion Clinic is granted in accordance with specific responsibilities and designated functions of each employee or collaborator
  - Outline in protocol!
- Training and or documentation required prior to access
  - Access and confidentiality agreements for employees and collaborators
  - Contracts for collaborators
  - Carilion Clinic Visiting Student Affairs process for onsite student collaborators
- Ensures compliance with HIPAA Privacy and Security Rule
- Access to Carilion Clinic PHI is a privilege, not a right.

Secure Data Sharing: Carilion Policy

- Carilion's Electronic Environments: **Epic, SPARC, REDCap, Secured Drives, TriNETx**
- Data storage and accesses required for all Investigators/Key Research Personnel must be defined in the protocol
- Principal Investigator's responsibility to ensure that only the minimum amount of access is requested for each Investigator/Key Research Personnel to accomplish the purpose of the study
- Continued access to Carilion's electronic environments requires a renewal process to ensure that approvals, personnel, level of access, and relevant training/agreements are up to date

Secure Data Sharing: Carilion Policy

- Duty to Promptly Report Privacy and Security Concerns:
  - Any researcher who identifies a potential HIPAA breach relating to research activities should notify the Carilion Clinic Privacy Office at privacy@carilionclinic.org (844)-742-6232 and the IRB of record as soon as possible
  - Carilion has time sensitive reporting obligations that are driven by the date a breach is discovered
  - A breach is treated as discovered as of the first day of which the incident is known to any Carilion workforce member or agent
- Privacy & Security Noncompliance = reputation risk, disciplinary action, epic access block, regulatory enforcement, sanctions, licensing board actions, HIPAA financial fines (up to $1.9 million), civil action, criminal penalties

Reliance Agreement

- Carilion has a **Memorandum of Understanding (MOU)** with Virginia Tech
  - MOU includes IRB reliance and IRB review responsibilities
- This formalized agreement includes reliance for exempt and non-exempt human subjects research

Early communications about study requirements are strongly recommended.

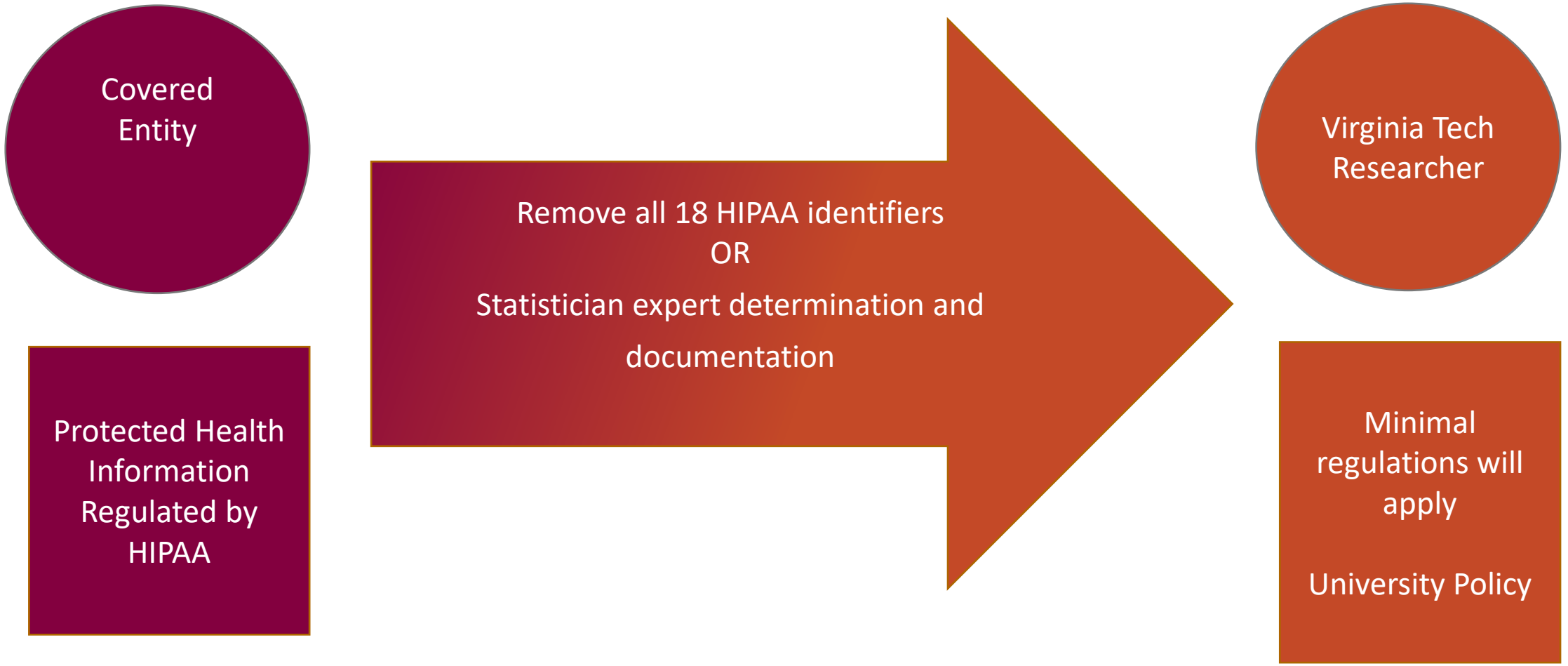
Carilion Clinic

Virginia Tech

VTC | Virginia Tech Carilion School of Medicine

Pathways for Moving Information From Covered Entity to Researcher

De-Identified Data



Limited Data Set

Covered Entity

Protected Health Information Regulated by HIPAA

Remove all HIPAA identifiers
EXCEPT
City, State, Zip codes and Dates

Data Use Agreement is executed between covered entity and Virginia Tech
-DUA must include specific provisions

Virginia Tech Researcher

Terms of Data Use Agreement
Federal Regulation (Common Rule)
University Policy
*Data are PHI

Signed Patient Authorization

Covered Entity

Protected Health Information Regulated by HIPAA

Patient signs authorization that includes core elements and required language. Signed authorization is documented and maintained by the covered entity.

Patient consents and enrolls in IRB-approved study

Virginia Tech Researcher

Information subject to state and federal regulations University Policy

HIPAA Waiver of Authorization

Covered Entity

Virginia Tech Researcher

<u>IRB must review and approve</u>

Research could not be practicably conducted without PHI

Research could not be practicably conducted without waiver

Disclosure involves no more than minimal risk to the individual

Adequate plan to protect identifiers from further disclosure

Adequate plan to destroy identifiers at earliest opportunity

Adequate assurance that PHI will not be reused or disclosed

Protected Health Information Regulated by HIPAA

Information subject to state and federal regulations University Policy

Waiver of HIPAA Criteria

The Carilion IRB/Privacy Board is allowed to grant a waiver of authorization if it can certify that the research meets the **following criteria**:

1. The use or disclosure of PHI involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements:
    - an adequate plan to protect the identifiers from improper use and disclosure;
    - an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
    - adequate written assurance that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of PHI would be permitted by this subpart;
2. The research could not practicably be conducted without the waiver or alteration; and
3. The research could not practicably be conducted without access to and use of the PHI

Outlined in 45 CFR 164.512(i)(2)(ii)

Decedent Research

Covered Entity

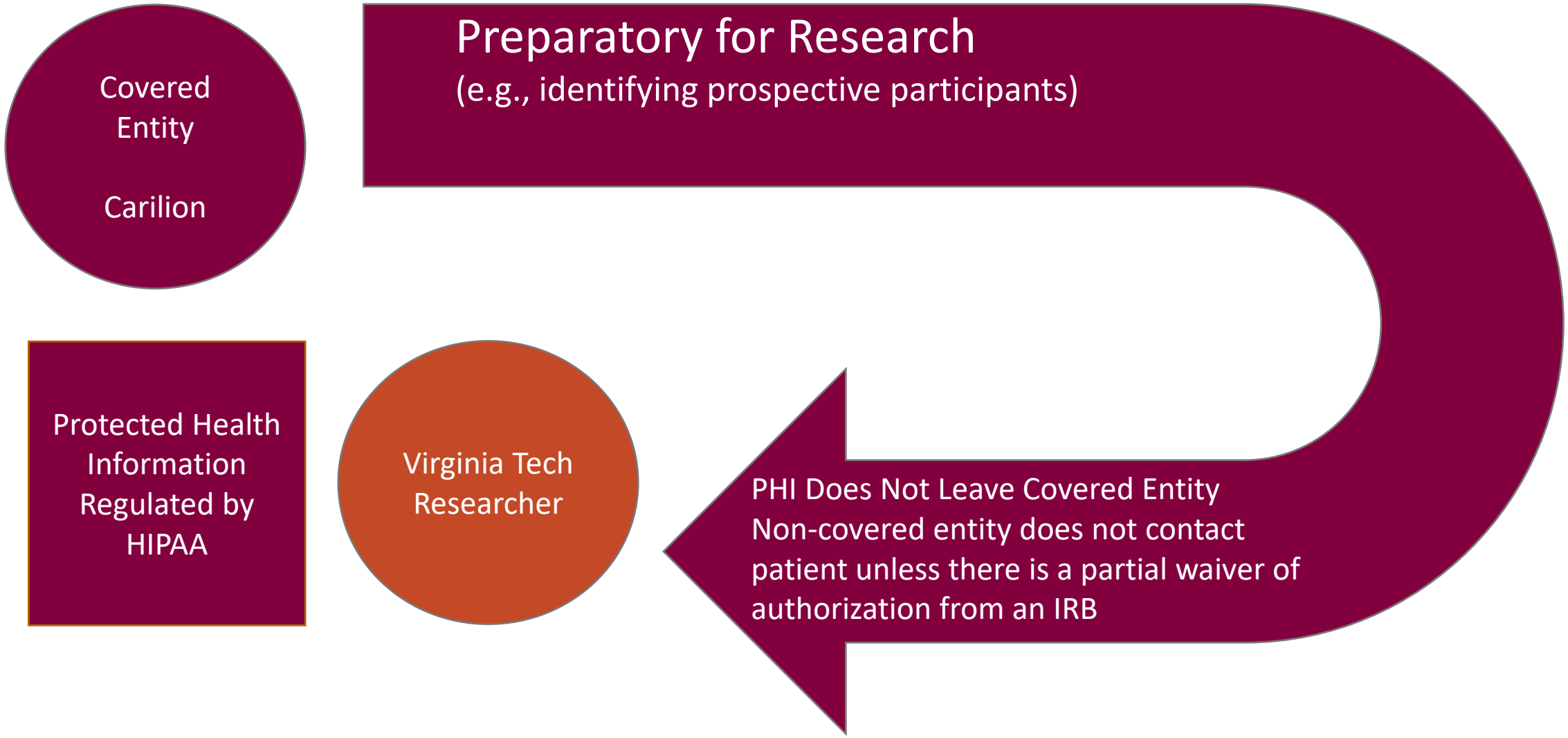
Protected Health Information Regulated by HIPAA

Use is solely for research
PHI Is necessary for research
Documentation of death

Virginia Tech Researcher

Information subject to state and federal regulations
IRB does not review
University Policy

Pathway for Covered Entity to Provide Researchers Access to Information



Pathways for Moving Information From Covered Entity to Researcher

*Not a recommended path for research at Virginia Tech

Planning purposes

- **Carilion IRB** has oversight authority for research involving Carilion patients, employees, or facilities.
- When **Carilion Clinic** will serve as the IRB of record:
  - Study team must proceed with the Carilion IRB submission process and requirements
  - Detailed information about external collaborators must be described in the Collaboration section [Section 9] within the IRB application
  - Only Carilion Clinic employees holding a full-time position may be designated as Principal Investigator (PI) or Co-Investigator

Frequently Asked Question

Q: I will be collecting survey data that asks people sensitive information about their health. Do the HIPAA regulations apply to my data?

A: No. We call this data Research Health Information (RHI). It is sensitive and does need to be protected. Federal regulations like the Common Rule, requiring IRB review and approval, regulate this type of data. State laws also protect certain types of health information.

Frequently Asked Question

Q: When is a researcher consider to be a covered healthcare provider under HIPAA?

A: A researcher is a covered health care provider if he or she furnishes healthcare services to the individuals, including the subjects of research, and transmits any health information in electronic form.

For example, a researcher who conducts a clinical trial that involves the delivery of routine health care, such as an MRI or liver function test, and transmits health information in electronic form to a third-party payer for payment, would be a covered health care provider under the Privacy Rule.

Frequently Asked Questions continued

Q: I am a Virginia Tech researcher with a joint appointment at Carilion. Are my research data Protected Health Information regulated by HIPAA or are they Research Health Information?

A: The determination of whether an individual researcher must comply with the HIPAA Privacy Rule is a fact-sensitive, individualized determination. This will depend on specific project details. Please consult with Carilion, Virginia Tech IRB and Virginia Tech Privacy and Research Data Protection Program (prdp@vt.edu)

Frequently Asked Question

Q: Can a researcher use or disclosure individual's protected health information for research recruitment purposes?

A: PHI can be disclosed for recruitment purposes if a HIPAA authorization has been obtained or a waiver of the HIPAA authorization requirement has been granted by the IRB. Treating providers may discuss with their own patients the option of enrolling in a study without a research HIPAA authorization or waiver. However, the treating provider may not disclose PHI to anyone else for purposes of recruitment in a research study without a HIPAA authorization permitted others to obtain the information.

Researchers who are not treating providers of potential subjects can request referrals of eligible patients from treating providers.

Frequently Asked Questions continued

Q: I will collect data using a software that says it is ‘HIPAA Compliant’. Should I make sure I tell my participants and sponsor that the study is ‘HIPAA Compliant’?

A: No. Telling participants that the data collected and processed by the research team are ‘HIPAA Compliant’ is misleading. If you read the fine print, you will see:

- “HIPAA compliant with respect to a covered entity”
- “We offer a platform that enables covered entities to collect and manage PHI through surveys while being compliant with HIPAA”
- “Be mindful that no software alone is truly compliant with any standard. It is the environment into which software is installed that can be called compliant”

Frequently Asked Question

Q: Can the preparatory research provision of the HIPAA Privacy Rule be used to recruit individuals into a research study?

A: The preparatory research provision permits covered entities to use or disclose protected health information for purposes preparatory to research, such as to aid study recruitment. However, the provision at 45 CFR 164.512(i)(1)(ii) does not permit the researcher to remove protected health information from the covered entity's site. A researcher who is an employee or a member of the covered entity's workforce could use protected health information to contact prospective research subjects.

Takeaway – a non-Carilion researcher (i.e. external collaborator) may not use the preparatory research provision to contact prospective research subjects.

Frequently Asked Questions continued

Q: Virginia Department of Health (VDH) provided me with an existing data set to analyze for research purposes. Is this data set regulated by HIPAA?

A: No. HIPAA establishes the conditions under which VDH can provide the dataset to researchers. Once Virginia Tech has the dataset, the terms of the data use agreement, and other federal and state laws are in place to protect the data.

*If Virginia Tech were to enter into a Business Associate Agreement with VDH, the data set would be regulated by HIPAA. This is not currently an option at Virginia Tech.

Frequently Asked Question

Q: If a research participant revokes their HIPAA authorization, can a researcher continue using the information?

A: The researcher may only continue to use and disclose protected health information that was obtained **prior** to the time the participant revoked their authorization, as necessary to maintain the integrity of the research study.

Navigate research: The Health Analytics Research Team (HART) has developed a resource to provide as much or little information as you need. Visit MyProjectPath for more in-depth information tailored to your specific project.

Project Types (Research, QA/QI)

RESEARCH AND INNOVATION

SCHOLARLY INTEGRITY AND RESEARCH COMPLIANCE

VIRGINIA TECH®