



University HIPAA Policy: What It Means for Your Research
Part I

June 2021



Why Create a University HIPAA Policy?

- **Opportunity to reinforce OSU's Mission**
- **Transparency**
 - Items not known to university community
 - Hybrid Covered Entity status
 - Mechanism of how the Med Center has been allowed to disclose PHI to the College of Medicine and other colleges related to research and HIPAA
 - OSU's HIPAA program not readily apparent to regulators
- Highlights existence of governance structures, such as the University Compliance & Integrity Council (UICC), as well as the Covered Health Care Components (CHCC) Committee
- Introduces new data definition, **Research Health Information (RHI)**, which is outside the jurisdiction of OCR enforcement
 - **Promote protections of research related data**
 - **Reduce regulatory exposure**



University HIPAA Policy Key Definitions

- **HIPAA:** Health Insurance Portability and Accountability Act (HIPAA) as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH), and its implementing regulations. HIPAA addresses Protected Health Information (PHI) that is created, received, maintained, or transmitted by a Covered Entity.
- **Covered Entity:** Organization that conducts certain types of transactions in electronic form and includes health plans, health care clearinghouses, and health care providers.
- **Hybrid Entity:** A single legal entity that performs covered and non-covered functions under HIPAA. OSU is a HIPAA hybrid entity.
- **Covered Component:** Divisions/units of a hybrid entity that perform functions covered under HIPAA.
- **Service Unit:** A university unit that creates, receives, maintains or transmits PHI **on behalf of** a health care component. The service unit is subject to HIPAA only as it is performing functions on behalf of a covered entity.

University HIPAA Policy Key Definitions-continued

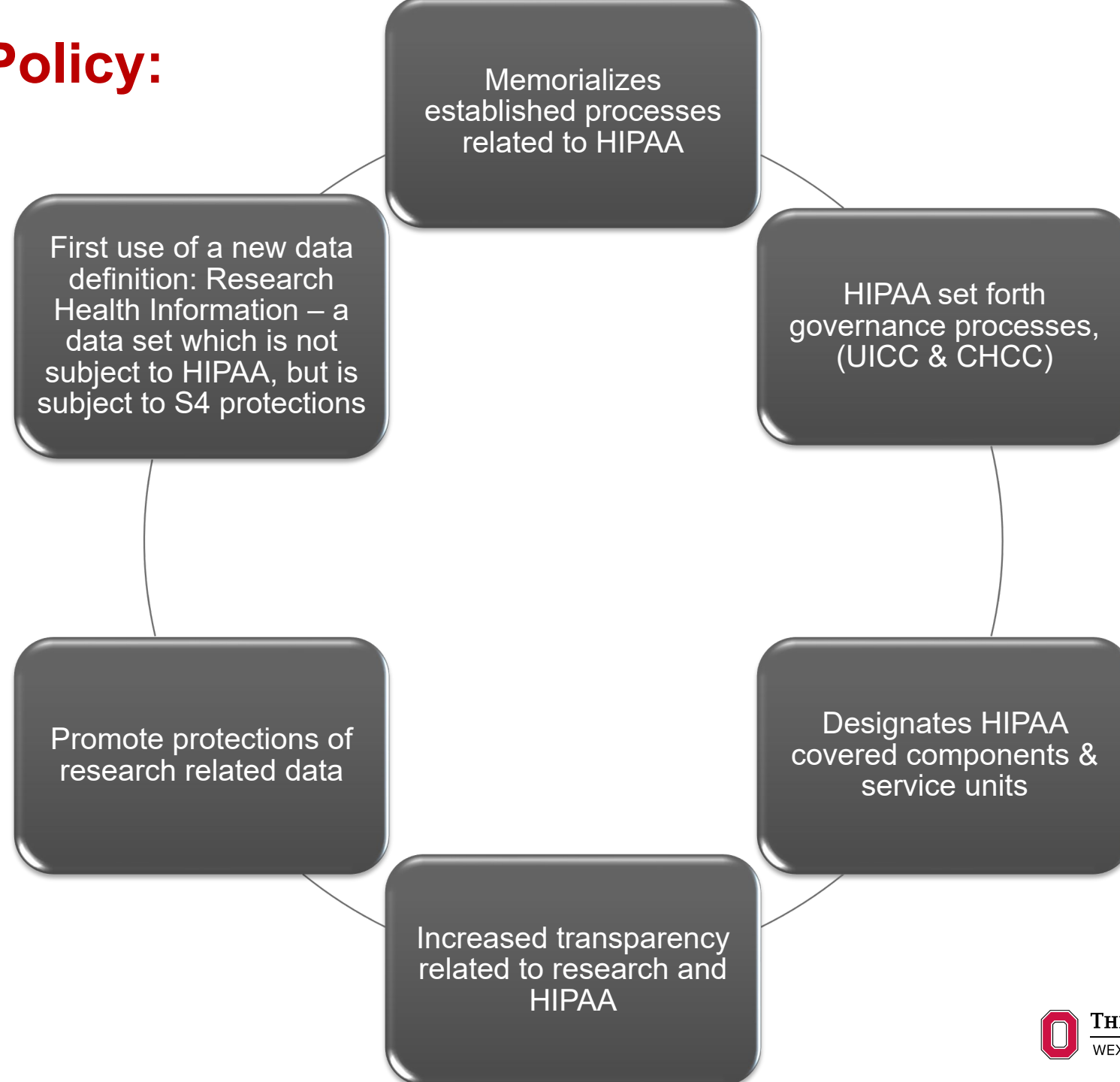
- **Protected Health Information:**

Individually identifiable information (oral, written, or electronic) that

- (1) is created or received by a covered entity or health care component and
- (2) relates to a patient's past, present, or future physical or mental health; the receipt of health care; or payment for that care. This includes the PHI of deceased individuals, unless the individual has been deceased for more than 50 years.

University HIPAA Policy:

What Does It Do?





Policy Statement

The university is a **covered entity** under HIPAA.




- More specifically, because the university is a multi-service organization that engages in both HIPAA-covered and non-HIPAA-covered activities, it has designated itself as a **hybrid entity**.
- This designation allows the university to limit its HIPAA obligations only to those **health care components** that perform HIPAA-covered services and the **service units** supporting them.

Who/What is the OSU HIPAA Hybrid Entity?



THE OHIO STATE UNIVERSITY HIPAA HYBRID ENTITY

COVERED FUNCTION	
<p>When performed by the units below, receiving, creating, or maintaining individually identifiable health information for the purposes of</p>	<ol style="list-style-type: none"> 1. treatment, 2. payment for health services, or 3. administrative healthcare operations (business, financial, legal, etc.) falls under the covered component of Ohio State's hybrid entity.
<p style="text-align: center;">Health care units</p> <ul style="list-style-type: none"> DENTISTRY MEDICAL CENTER NISONGER OPTOMETRY OSU HEALTH PLAN OSU PHYSICIANS, INC. WILCE STUDENT HEALTH 	<p style="text-align: center;">Service units</p> <ul style="list-style-type: none"> Business & Finance College of Medicine College of Nursing College of Pharmacy Corporate Engagement Office Department of Internal Audit Office of Administration & Planning Office of Chief Information Officer Office of Human Resources Office of Institutional Equity Office of Legal Affairs Office of University Compliance & Integrity Uniprint University Facility & Operations University Office of Advancement University Risk Management

NON-COVERED FUNCTION
 <p>Activities performed by all other colleges and units</p>
 <p>Activities performed by the units listed at left that are not related to treatment, payment, or administrative healthcare operations</p>
 <p>Research <i>(Data may be subject to HIPAA)</i></p>





Who Does This Policy Apply To?

If your role at OSU includes use of protected health information, the policy applies to you.

- i.e.
 - University Covered Component Workforce
 - University Service Unit Workforce
 - OSU Researchers Who Use PHI For Research Purposes



Respecting Patient Privacy

- Behind any dataset, there are patients/subjects.
- We believe that every piece of a patient's medical information is private and deserves protection.

Absent any policy or regulation, always remember that OSU faculty, staff, and students must respect the privacy of patients and study subjects



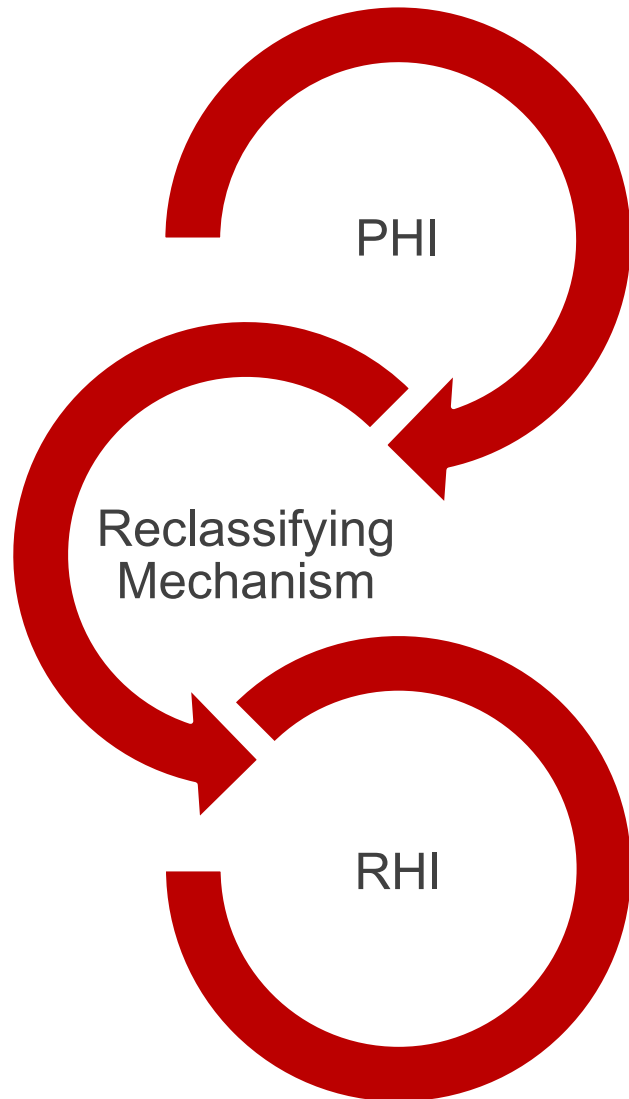
Research Health Information

Information collected about research subjects that pertains to their health or healthcare which either:

- 1) is created or received in connection with research that does not involve a covered health care component or
- 2) has been reclassified and is no longer subject to HIPAA requirements due to a disclosure from a health care component pursuant to a valid HIPAA research disclosure, such as a valid authorization or a full or partial waiver of HIPAA research authorization.

RHI → Stored outside of the EMR

PHI → RHI



What are the reclassifying mechanisms?

1. Signed written authorization
2. Valid partial HIPAA authorization
3. Valid full HIPAA authorization

Approved sources, such as HBOC or the Information Warehouse are authorized to provision data which is re-classified. Individual PIs may not re-classify data on their own

Disclosure of PHI and Minimum Necessary

Permitted Uses and Disclosures. A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization, for the following purposes or situations: (1) To the Individual (unless required for access or accounting of disclosures); (2) Treatment, Payment, and Health Care Operations; (3) Opportunity to Agree or Object; (4) Incident to an otherwise permitted use and disclosure; (5) Public Interest and Benefit Activities; and (6) Limited Data Set for the purposes of research, public health or health care operations.¹⁸ Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.



A covered component is permitted, but not required to disclose PHI for research activities.

RHI Data Classification

- OSU University Institutional Data Policy protects RHI as **S4 (restricted)** institutional data which requires the highest levels of protections outlined in the Information Security Control Requirements (ISCR)
- Required protections are outlined in the Risk Management Framework (IRMF) and Information Security Control Requirements (ISCR)

The full framework can be found here:

<https://cybersecurity.osu.edu/cybersecurity-ohio-state/internal-policies-compliance/security-framework>

RHI Data Protections

Researchers are responsible for protecting Research Health Information. Some ways that RHI is protected include, but are not limited to:

- Multi- Factor Authentication
- Encryption
- Unique User Accounts
- Minimum Necessary Access
- Access Auditing

Your IT Department and Security Coordinator will help ensure the appropriate controls for your use case are identified and met.

Data Protection Plans:

Compliance with S4 Protections

- It is important that RHI is properly protected and a research data protection plan is in place **prior** to using/storing RHI
- **Reach out to your designated IT Security team for assistance in developing a compliant plan:**
 - Security Coordinators:** <https://cybersecurity.osu.edu/SecurityLiaisons>
 - Covered Component Privacy and Security Officers:** <https://it.osu.edu/sites/default/files/2019/09/hipaa-privacy-and-security-officer-contact-list-u190923.pdf>
- Researchers aren't required to know all of the controls, but should be familiar with the framework and then work with their IT Departments and Security Coordinators to:
 - Identify appropriate storage and technologies for use and storage of RHI
 - Properly evaluate any new software or cloud applications for use with RHI

Criteria For Obtaining Patient Data For Research

- Covered component policy applies.
- For example, as OSUWMC, there must be an OSU credentialed faculty member on the study team, and a
- HIPAA authorization or a waiver of authorization from an IRB/Privacy Board.

HIPAA Waivers & Alterations of HIPAA Authorization

- HIPAA research authorization: signed permission by the patient to use/disclose their information for research purposes
- HIPAA waivers of authorization are approved by the IRB to waive the requirement for patient authorization for use/access/retention of PHI for research purposes

Partial Waiver

- Allows PHI access/retention to identify potential subjects (i.e., recruitment). Information must be destroyed after recruitment is complete

Full Waiver

- Allows PHI access/retention without authorization for entire research study (e.g., retrospective chart review)

In general, if a study involves prospective access to patient information, written authorization should be obtained.

Example of Covered Component Policy on De-identification of PHI

Per OSUWMC policy:

- Researchers should request **de-identified** datasets whenever possible. Methods to de-identify are limited to:
 - De-identification of PHI:
 - All 18 elements of PHI are removed from the dataset
 - Researchers may de-identify datasets if:
 - the process described in the IRB submission and approved by the IRB, and
 - the de-identification is validated by Information Security
 - Expert determination certifying that the statistical risk is miniscule that the data could be re-identified.
 - Expert determination requires a qualified third party
 - Researchers may not de-identify and provide their own expert determination
- No IRB approval is needed when requesting de-identified data from the Information Warehouse (IW)

Identifying & Recruiting Potential Participants

IRB and OSUWMC policy prohibits cold calling of potential research participants.

OSUWMC HIPAA Research Policy:

- *The research team must not cold call potential subjects; investigators must coordinate with a treating clinician before contacting the potential subject.*
- *Recruitment scripts must contain a link between treating clinician and investigator.*

Use Case #1:

RHI or PHI?

- ❑ **Q:** *A OSUWMC IW provided a data set to a PI pursuant to a HIPAA waiver. The PI was conducting a retrospective study. A member of the study team downloaded a portion of the data from a secured OSU server to an unencrypted laptop. The laptop was lost. Someone unaffiliated with OSU contacted OSU security with questions about the individuals identified in the data set. Is the data considered RHI or PHI?*

- ✓ **A:** The data is RHI. PHI was reclassified as RHI when the data was disclosed/released from the covered component pursuant to an IRB HIPAA waiver. Although the information derived from patient care, the release/disclosure, by policy, makes the data RHI. The researcher failed to follow several security policies.

Use Case #2:

RHI or PHI?

- ❑ **Q:** *A researcher is conducting a therapeutic clinical trial pursuant to patient consent and the patient's HIPAA authorization. Is the information I am gathering and entering into the electronic medical record (EMR) RHI or PHI?*

- ✓ **A:** Patient information generated in a therapeutic clinical trial is PHI when entered into an EMR for the purposes of treatment or clinical care; the data is being used for patient care within the covered component and is therefore subject to HIPAA.



When to Report

- Under HIPAA and university policy, all inappropriate disclosures of data must be reported
- Inappropriate disclosure = compromise of patient confidentiality

Examples:

- Lost/theft of laptop, flash drive, or other device
- Loss of paper documents
- Misdirected email



Where to Report: *Incidents Involving PHI*



- Follow departmental procedure for reporting incidents involving PHI
- Contact your designated Privacy or Security official to report an incident
- If you do not have a designated Privacy Official, PHI incidents may be reported to the OSUWMC Privacy Office at (614) 293-4477 or PrivacyOffice@osumc.edu



Where to Report:

Incidents Involving RHI



- Contact your designated Privacy or Security official to report an incident
- Follow departmental procedure for reporting incidents involving university data
- RHI incidents should ultimately be reported to University Information Security
- Incidents involving research data may also need to be reported to the IRB via an Event Report

HIPAA Training

Who It Applies To:

- University researchers who receive RHI derived from PHI

Purposes Of Training:

- There are two reasons why a covered component may require a university researcher to complete HIPAA training prior to disclosing patient data for research:
 - 1) To ensure the researcher understands that the health information they receive is **derived** from a person whose information **must be safeguarded** and honored as private regardless of its classification as PHI or RHI.
 - 2) To provide additional assurance to the covered component, as steward of patient data, that privacy and confidentiality will be protected after disclosure to the researcher.

Thank You



wexnermedical.osu.edu



THE OHIO STATE UNIVERSITY

University HIPAA Policy

Part 2: RHI case examples & Buck-IRB tips



Key takeaways:

RHI is a new term/data classification, but

- ✓ **Continue** to obtain authorization or request waivers of HIPAA auth if your research accesses, uses, or creates PHI*
- ✓ **Continue** to protect health-related research data
- ✓ **Consider** source of data when completing Buck-IRB application
- ✓ **Identify** where to report breaches

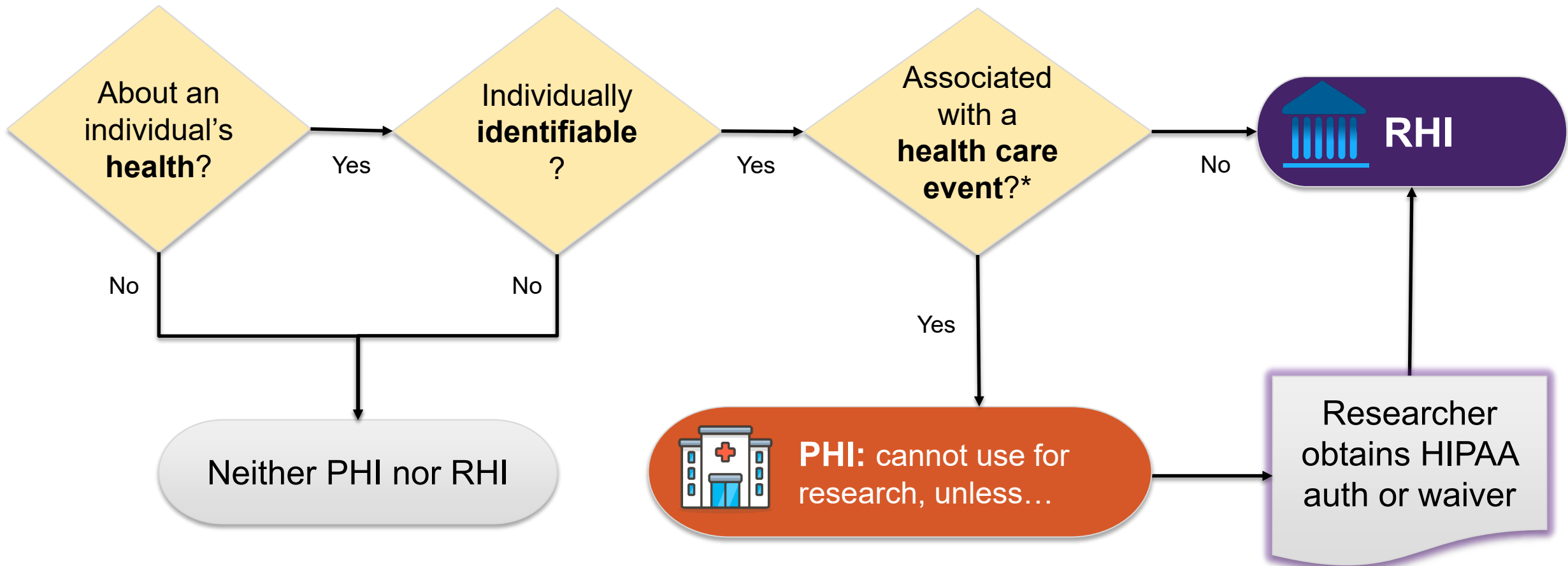


**Refer to ORRP Education Session on waivers of consent & HIPAA (2019) for more details*



RHI or PHI?

Does the research involve **accessing, using, or creating** materials that are:



* i.e., obtained from or held by a covered entity/component



Buck-IRB

Is individually identifiable Protected Health Information (PHI) subject to the [HIPAA Privacy Rule](#) requirements to be accessed, used, or disclosed in the research study?*

Yes

No



Select **YES** to this question when:

- the source of materials is related to a treatment event/operations (medical records, clinic schedules), or
- the study generates data used for treatment in the context of clinical care.

→ Buck-IRB will then prompt you to identify the appropriate HIPAA-compliant mechanism for reclassifying the data as **RHI** (written authorization, full waiver, partial waiver, or alteration)



EXAMPLE 1

What do you think?

Scenario: Dr. Jones plans a study evaluating clinical outcomes of chemoradiation in lung cancer patients. He and his team will request data from radiation oncology medical records of patients who received this treatment between 2016 and 2020.

Question: In Buck-IRB, should Dr. Jones mark “Yes” to the question asking whether his study involves **PHI**?





EXAMPLE 1

What do you think?

Scenario: Dr. Jones plans a study evaluating clinical outcomes of chemoradiation in lung cancer patients. He and his team will request data from radiation oncology medical records of patients who received this treatment between 2016 and 2020.

Answer: Dr. Jones should mark “**Yes**” to the question asking if the study involves PHI because the data source is **health-related, identifiable,** and from a **covered component**. He must indicate which **HIPAA-compliant method** he will use to reclassify the data as RHI for research use



What do you think?

Scenario: Dr. Li, a psychology professor, plans to study brain activity in subjects with previously diagnosed traumatic brain injury (TBI). Participants will undergo fMRI at the Center for Cognitive and Behavioral Brain Imaging (CCBBI), and the radiological images will be used to identify areas of the brain that are activated in response to an audio stimulus.



EXAMPLE 2a

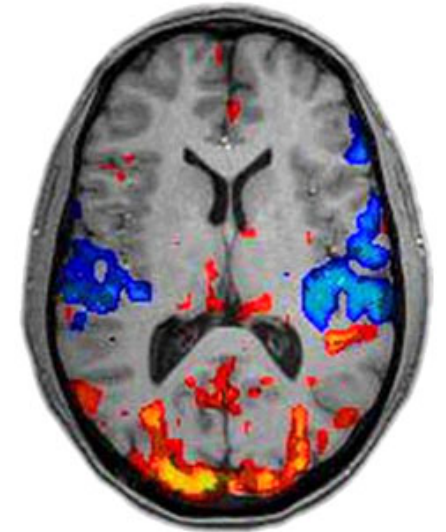
Question: Does this study involve **PHI**, **RHI**, both, or neither?

What do you think?

Scenario: Dr. Li, a psychology professor, plans to study brain activity in subjects with previously diagnosed traumatic brain injury (TBI). Participants will undergo fMRI at the Center for Cognitive and Behavioral Brain Imaging (CCBBI), and the radiological images will be used to identify areas of the brain that are activated in response to an audio stimulus.

Answer: This study involves **only RHI**. Although fMRI images constitute **identifiable health information**, the information is not held or transmitted by a covered entity. The scans are conducted for research and are not used for clinical purposes. Therefore, the research data is **RHI**.

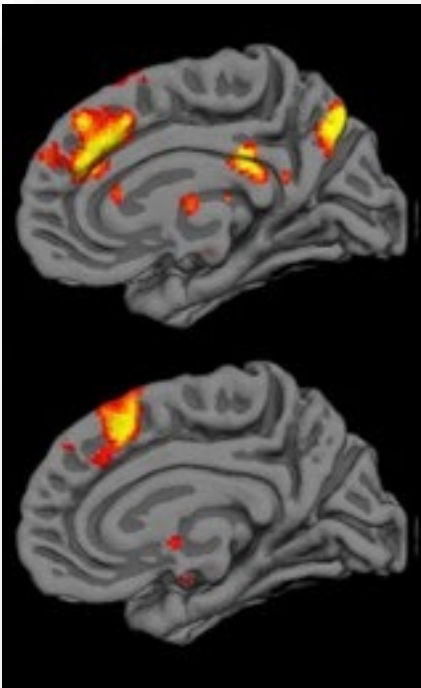
EXAMPLE 2a





EXAMPLE 2b

What do you think?



Scenario: Dr. Li, a psychology professor, plans to compare brain activity in subjects with previously diagnosed TBI and **healthy controls**. Participants will hear an audio stimulus while undergoing fMRI.

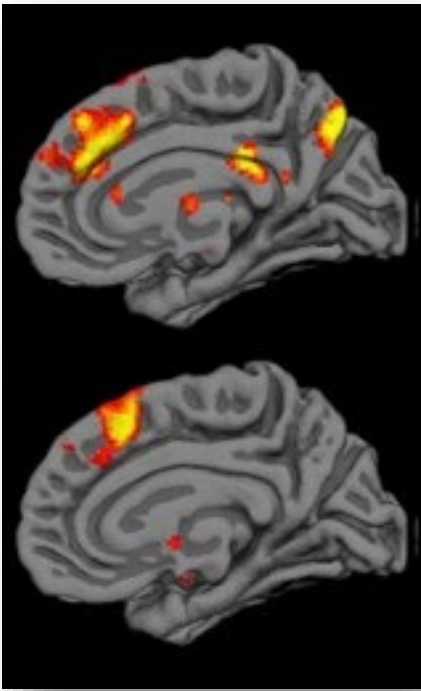
A neuro-radiologist will clinically evaluate each scan and notify subjects' physicians if an abnormality is identified; the costs of the clinical evaluation will be billed to the research team.

Question: Does this study involve **PHI**, **RHI**, **both**, or **neither**?



EXAMPLE 2b

What do you think?



Scenario: Comparison of brain activity in subjects with previously diagnosed TBI and **healthy controls**. Participants will hear an audio stimulus while undergoing fMRI.

A neuro-radiologist will clinically evaluate each scan for abnormalities; the costs of clinical evaluation billed to research team.

Answer: This study generates **both RHI** and **PHI**.

The fMRI images (**identifiable health information**) become **PHI** when the neuroradiologist **clinically evaluates** the images and when images are sent to clinicians for treatment follow-up (also members of **covered entities**).



EXAMPLE 3a

What do you think?

Scenario: Dr. Singh, a surgical oncologist, wants to study quality of life of breast cancer patients in remission.

- Recruitment via flyers posted in clinic waiting area where she works
- Questionnaires at two time points that ask about current medications, comorbidities, daily activities, and general health and wellness
- Identifiers will be retained in order to link survey responses

Questions: (1) Does the study involve **PHI**?
(2) Should the PI request HIPAA authorization/
waivers to reclassify as **RHI**?





EXAMPLE 3a

What do you think?

Scenario: Survey study collecting info about current medications, comorbidities, daily activities, and general health and wellness. Identifiers will be retained. Subjects recruited via flyers.

Answers:

(1) No, PHI is not involved in this study. Although Dr. Singh will collect **health information** that includes **identifiers**, the source of that information is the subjects themselves, not a covered entity. Therefore, the study involves only **RHI**.

(2) HIPAA authorization/waivers are not needed (only consent).





EXAMPLE 3b

What do you think?

Scenario: To increase enrollment into her QOL study, Dr. Singh proposes a change in her recruitment method:

- Instead of posting flyers, she will directly recruit patients she sees in the clinic; **she will review her clinic schedule to identify eligible subjects**
- The rest of the study is unchanged (2 questionnaires, identifiers retained)

Questions:

(1) Does the study involve **PHI**?

(2) Should the Dr. Singh request HIPAA authorization/waiver to reclassify data as **RHI**?





EXAMPLE 3b

What do you think?

Scenario: Survey study collecting info about current medications, comorbidities, daily activities, and general health and wellness. Identifiers will be retained. Subjects recruited from clinic schedules.

Answers:

(1) Yes, the study involves **PHI**. During recruitment, Dr. Singh will access identifiable health information that is held by a **covered entity**.

(2) A **partial waiver** is required in order to use PHI for research recruitment; once the partial waiver is in place, the **recruitment data set is RHI**.





Buck-IRB tips: waiver pages

List the source(s) of PHI applicable to the waiver (e.g., OSUWMC Information Warehouse, eResults, physician's office records, clinical database, etc.). Be as specific as possible.*

- ✓ Be specific – Information Warehouse, Dept. of X clinic schedules, etc.

Select all study team members who will access medical information:*

Erin Odor

- ✓ List only those team members who will access source documents that are PHI (e.g., IHIS, schedules, etc.)



What do you think?

EXAMPLE 4a

Scenario: Dr. Garcia is planning a secondary use study of identifiable health data.

- Data source: existing, IRB-approved research repository, which collects EMR data with participants' consent & HIPAA authorization
- Dr. Garcia will obtain waiver of the consent process



Question: Should Dr. Garcia also request a **waiver of HIPAA research authorization** to use data from the research repository in his secondary use study?

What do you think?

EXAMPLE 4a

Scenario: Dr. Garcia is planning a secondary use study of identifiable health data.

- Data source: existing, IRB-approved research repository, which collects EMR data with participants' consent & HIPAA authorization
- Dr. Garcia will obtain waiver of the consent process

Answer: No, Dr. Garcia should not request a waiver of HIPAA research authorization because **PHI is not involved** in this secondary use study.

The research repository data has already been reclassified as **RHI** through the *repository's* IRB protocol & HIPAA authorization process





What do you think?

EXAMPLE 4b

Scenario: Dr. Garcia is planning a secondary use study of identifiable health data from an IRB approved repository.

- He needs additional data points not held by the repository, so he plans to use identifiers from the repository to obtain additional info from medical records



Question: Does this change require additional HIPAA considerations?



What do you think?

EXAMPLE 4b

Scenario: Dr. Garcia is planning a secondary use study of identifiable health data from an IRB approved repository.

- He needs additional data points not held by the repository, so he plans to use identifiers from the repository to obtain additional info from medical records



Answer: Yes. The study now requires a **waiver of HIPAA research authorization** because the additional data points have not yet been reclassified as **RHI** via a HIPAA-compliant mechanism.

The Buck-IRB waiver request should only identify the new data points as **PHI**, as the original repository data has already been reclassified.



Buck-IRB: Confidentiality page

Explain how information is handled, including storage, security measures (as necessary), and who will have access to the information. Include both electronic and hard copy records.*

- ✓ Address protection of research data **regardless** of whether it is coming from a PHI source or not (i.e., address both types of **RHI**)
- ✓ Address protections **during all aspects of the study**—recruitment, collection, analysis, and transfer/sharing, if applicable.
- ✓ RHI must be protected to **S4** standards.



S4 Data Security

What options are available for RHI data storage?



Information Security

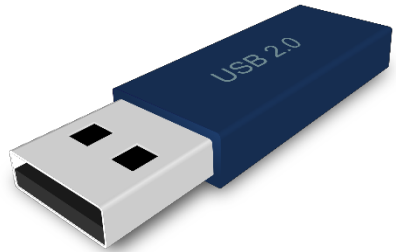
- Business Continuity Plans
- Critical Infrastructure Plans and Diagrams
- External, non-credentialed vulnerability scan results
- Information Security Investigative Data
- Internal, credentialed vulnerability scan results
- Merchant IDs
- Network and System Diagrams and Configurations
- Non-Public Network Addresses
- Password, Private Encryption Key, and Identity Management Database or Repository
- Research Health Information (RHI)
- Risk and Information Security Assessments

- Visit OCIO’s **Institutional Data Calculator** to generate a list of approved services/apps
- Covered components may require **additional protections** as a condition of releasing PHI for research
- If it is not feasible to use an approved platform, option to **request an exception** through department IT – stay tuned!



EXAMPLE 5

What do you think?



Scenario: Dr. Hoar, an English professor, is conducting a study on narratives of health. As part of the project, he obtains HIPAA research authorization to obtain data from subjects' medical records in order to correlate narratives with diagnoses. A research assistant saves a copy of the medical data on an unencrypted flash drive and then loses the flash drive.

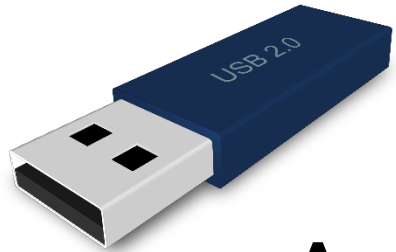
Questions:

- (1) Does this represent a breach of **PHI**, **RHI**, or **neither**? Why?
- (2) What actions should the PI take?



EXAMPLE 5

What do you think?



Scenario: Health information lost by researcher in English department.

Answers:

- (1) The loss of subject data is a breach of **RHI**, not PHI, because the information was not held by a covered entity. Although the source of the data was PHI, it lost that designation once subjects authorized its disclosure to the English department researchers.
- (2) The PI should notify his department's **IT Security contact**—not the HIPAA Privacy Officer—and submit an **Event Report** to notify the IRB of the protocol deviation & potential risks to subjects.

