

Learn More: *HIPAA*

RESEARCH ADMINISTRATION

December 2016

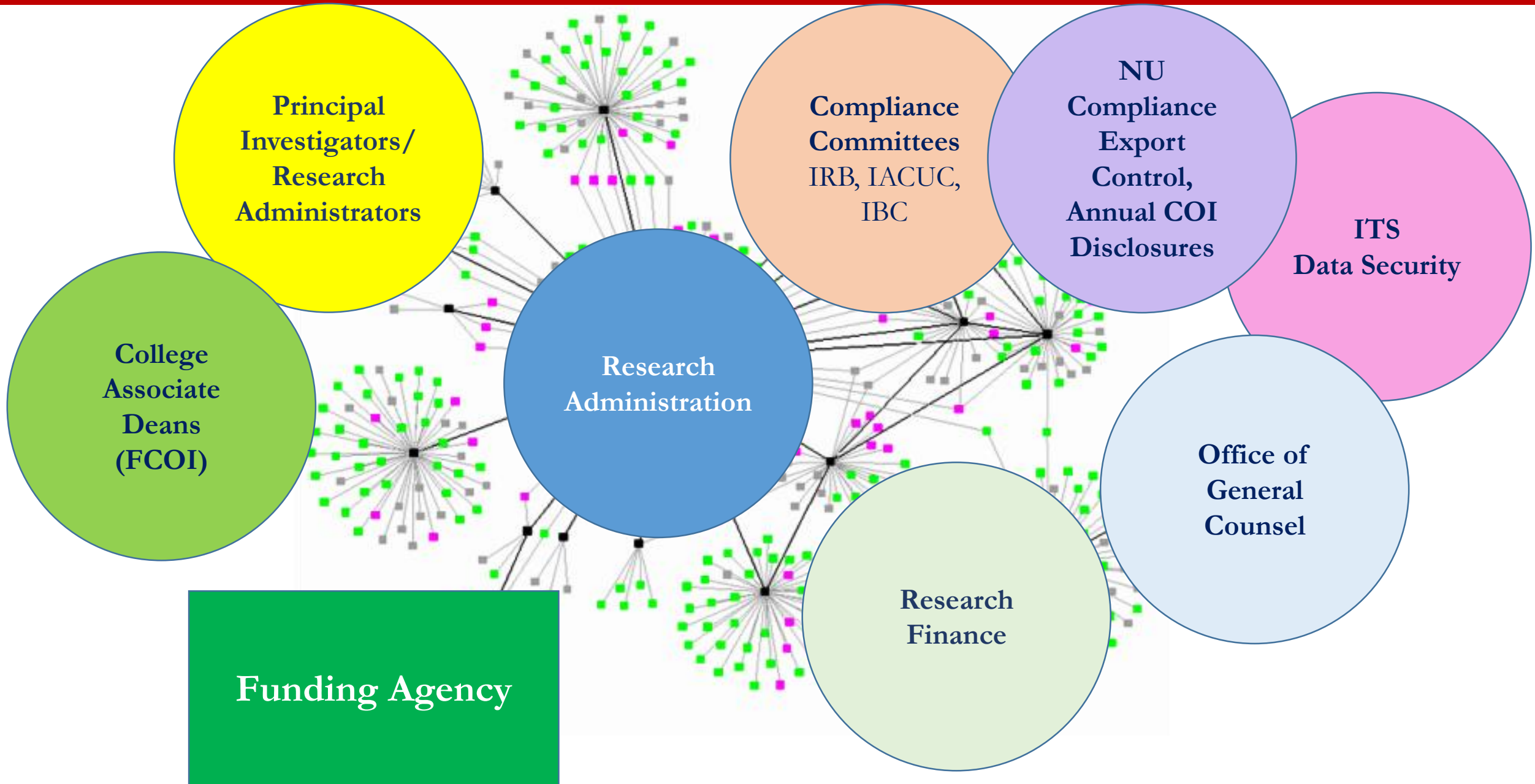
Learning Objectives

- Understand Research Administration's role in verifying that investigators and Northeastern University have complied with the awarding agency's requirements related to the HIPAA Privacy Rule.
- Understand the distinction between Protected Health Information (PHI) and Personally Identifiable Information (PII) and what constitutes de-identified data.
- Understand the classification of research versus health services research versus operational services provided to a Covered Entity.
- Understand which agreements are needed to conduct research involving PHI – e.g., Data and Limited Data Use Agreements versus Business Associate Agreements.
- How you can help facilitate the process.

Institutional Certifications and Assurances

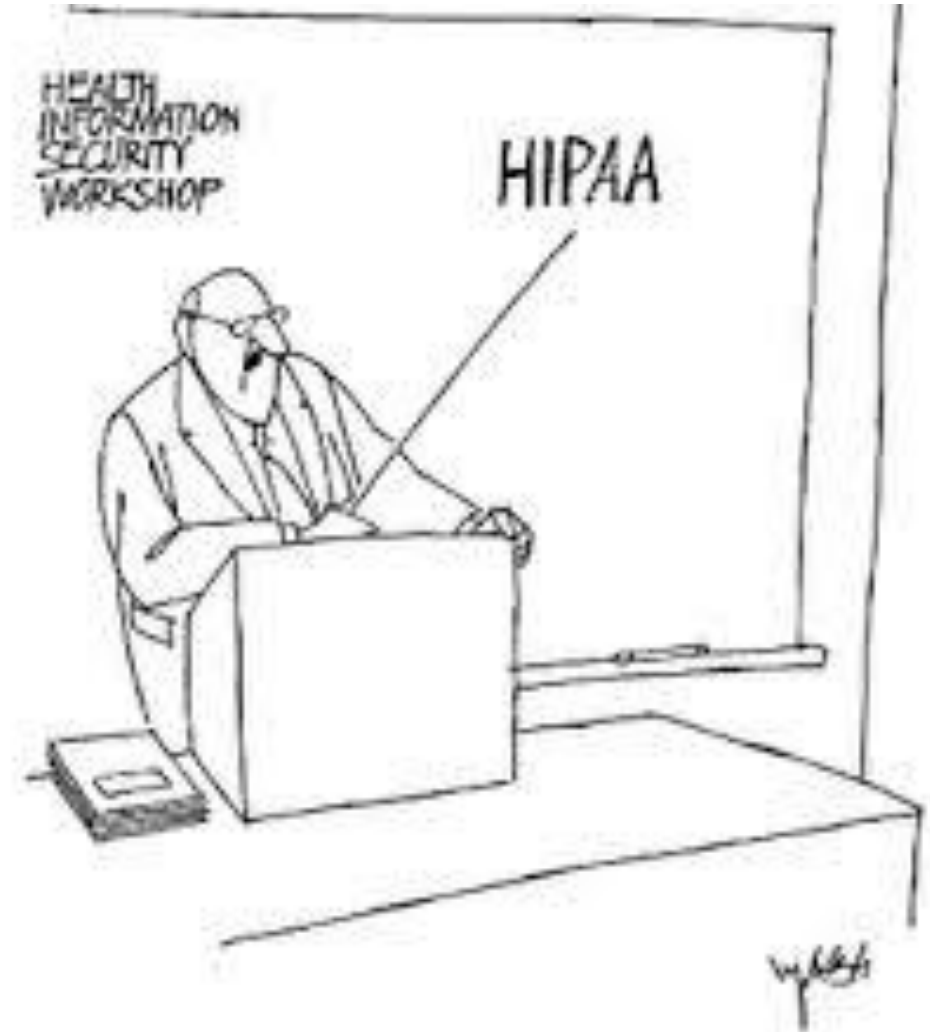
- Northeastern University, as a grantee, provides at the time of proposal submission and throughout the life-cycle of an award certification and assurances that it is in full compliance with all relevant laws, rules and regulations.
- How each grantee implements its research management responsibilities varies but all grantees should include documented practices that address specific regulatory requirements.
- Some regulations required that the grantee monitor the research activity; monitoring involves verification and tracking of compliance with a specific term or condition of the award.

Northeastern University



HIPAA KEY CONCEPTS

- The Health Insurance Portability and Accountability Act (HIPAA);
- Covered Entity;
- Privacy Rule; and
- Protected Health Information (PHI)



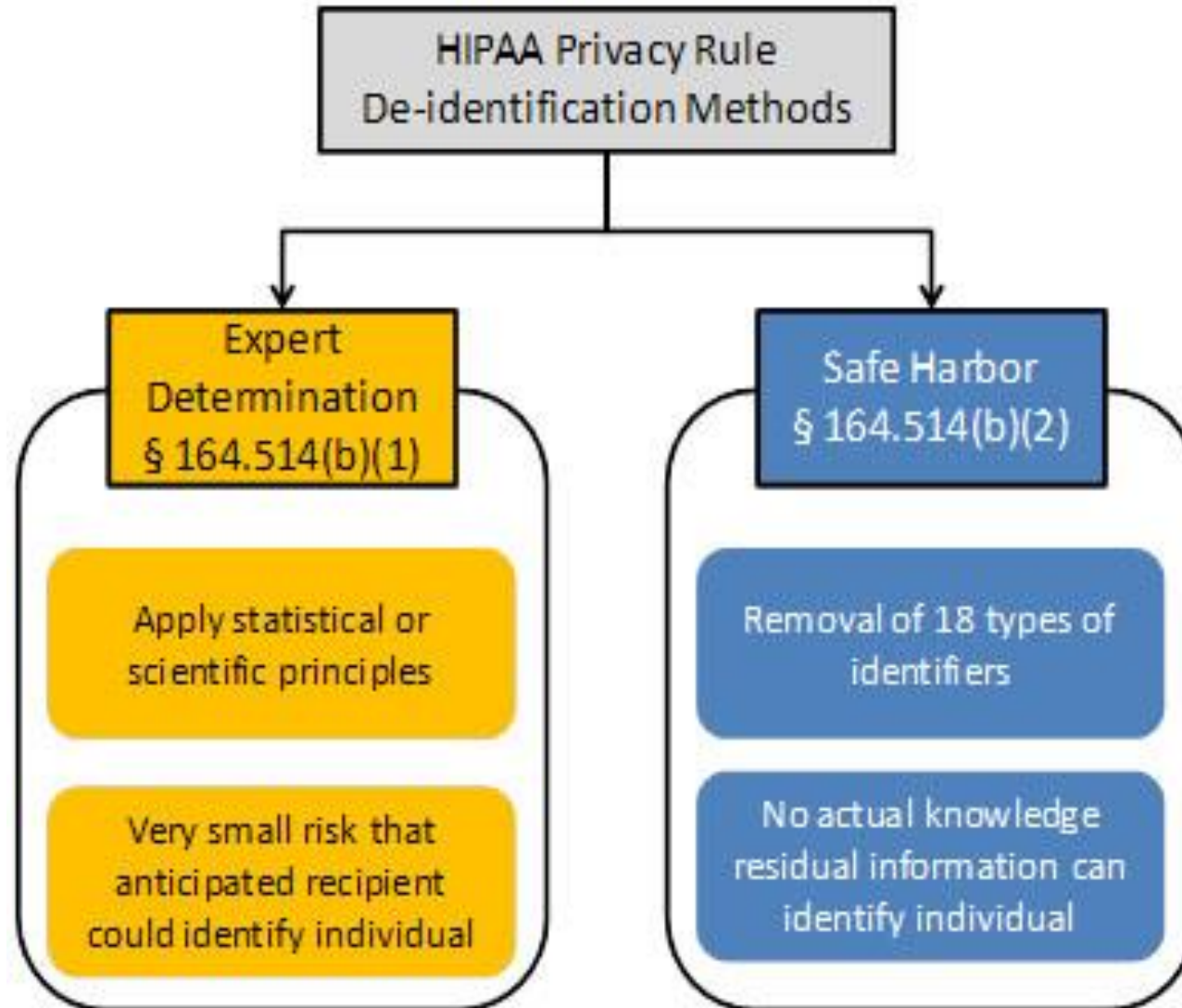
"No, it's not a female Hippopotamus, anyone else know?"

HIPAA

HIPAA is the acronym of the **Health Insurance Portability and Accountability Act** of 1996, which was a pre-cursor to the Affordable Care Act. The main **purpose** of this federal law was to help consumers maintain their insurance coverage but provisions also were included to **protect an individual's medical information.**

HIPAA required the US Department of Health and Human Services (DHHS) to adopt **standards regarding the electronic exchange, privacy, and security** of health information.

DE-IDENTIFIED DATA



HIPAA COVERED ENTITIES

Covered Entity:

Health Plans, Providers or Clearinghouses that **electronically transmit** health information.

HIPAA & THE PRIVACY RULE

Privacy Rule

The Privacy Rule defines what information needs to be protected (this is “protected health information”) and who can authorize a access the protected health information. The Privacy Rule delineates individuals' rights to the control and access of their PHI.

PROTECTED HEALTH INFORMATION

Protected Health Information (PHI): The HIPAA Privacy Rule protects most “individually identifiable health information” **held or transmitted by a covered entity** or its business associate...The Privacy Rule calls this information *protected health information* (PHI). Protected health information is information, including demographic information, which relates to:

- the individual’s physical or mental health or condition,
- the provision of health care to the individual, or
- payments for the provision of health care to the individual, and
- This information identifies the individual or for which there is a reasonable basis to believe can be used to **identify the individual**.

PROTECTED HEALTH INFORMATION

1. Names
2. Geocodes/Addresses
3. Dates related to an individual (DOB) or his or her medical care (appointments)
4. Telephone #s
5. Licenses
6. Vehicle identifiers/Plates
7. Fax #
8. Device identifiers and serial #
9. Email addresses
10. Web Universal Resource Locators (URLs)
11. Social security numbers
12. Internet Protocol (IP) addresses
13. Medical record numbers
14. Biometric identifiers, including finger and voice prints
15. Health plan beneficiary numbers
16. Full-face photographs and any comparable images
17. Account numbers
18. **Any other unique identifying number, characteristic, or code.**

HIPAA AND THE IRB

Area of Distinction	HIPAA Privacy Rule	HHS Protection of Human Subjects Regulations Title 45 CFR Part 46	FDA Protection of Human Subjects Regulations Title 21 CFR Parts 50 and 56
Identifiable Information	Defines PHI as individually identifiable health information that is transmitted or maintained in any form or medium (electronic, oral, or paper) by a covered entity or its business associates, excluding certain educational and employment records.	Private information must be individually identifiable in order for obtaining the information to constitute research involving human subjects. Individually identifiable means the identity of the subject is or may readily be ascertained by the investigator or associated with the information.	Title 21 CFR Parts 50 and 56 do not define individually identifiable health information.

PERSONALLY IDENTIFIABLE INFORMATION

Personally Identifiable Information (PII): "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

Privacy and security laws are designed to protect PII but may not necessarily involve requirements about the use of such data in research.

RESEARCH & SPONSORED ACTIVITIES

Research: is the “systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.” See 45 CFR 164.501.

Health Services Research involves projects designed to inform the quality of health care, reduce its cost, improve patient safety, decrease medical errors, or broaden access to essential services.

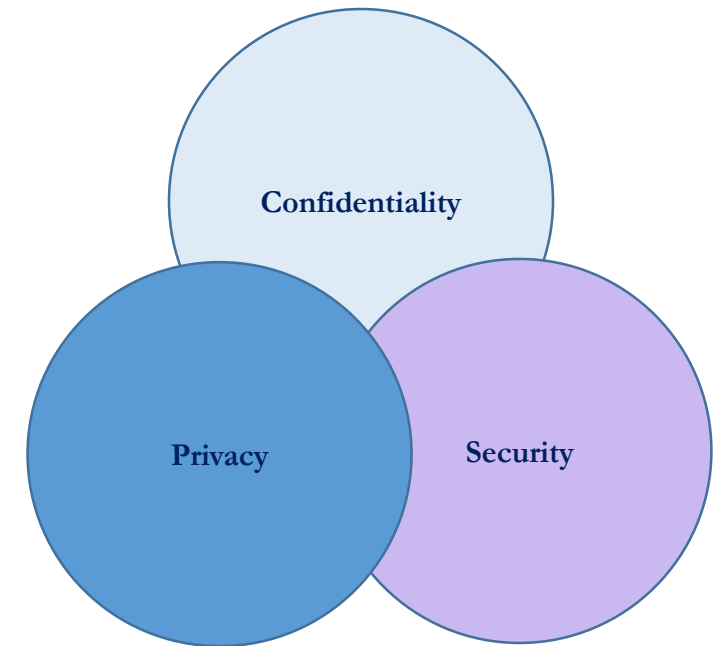
Business Associate activities are services performed by non-employees on behalf of a Covered Entity. **Business Associate Agreement (BAA)** is a contract between the Covered Entity and the BA and includes provisions designed to protect PHI.

HIPAA RELATED AGREEMENTS

Limited Data Use Agreement: an agreement that covers the transfer of a limited data set of protected health information.

Data Use Agreement: is an agreement between a provider and recipient that involves the use of PHI or PII.

Business Associate Agreement: A contract for services, e.g., patient billing, between a Covered Entity and a contractor.



ACTIVITIES & AGREEMENTS

	Agreement	Individual Authorization	IRB Review
Research	Data or Limited Data Use Agreement	Yes, Waiver or Alteration	Required
Health Care Operations Activity/Research	Data or Limited Data Use Agreement	Yes, Waiver or Alteration	HSDF
Contracted Services	Business Associate Agreement	No	Not Required

Reminder: The de-identification of PHI data takes it outside of the Privacy Rule; no data use agreement is required.

RESEARCH ADMINISTRATION

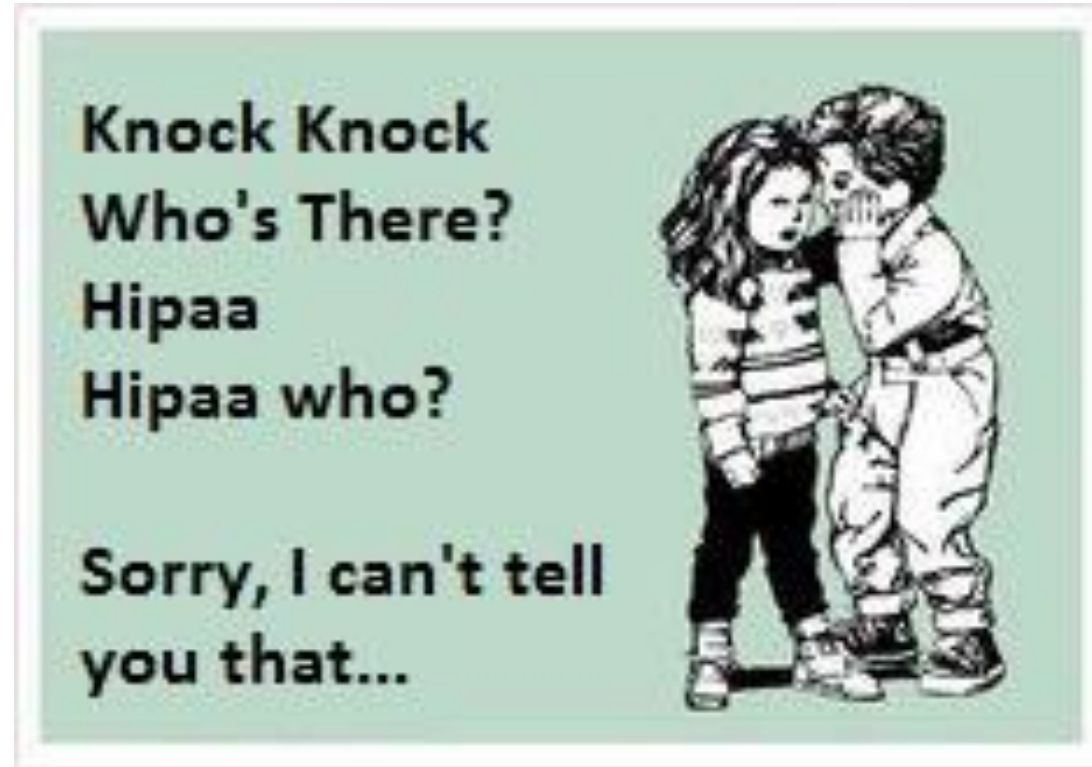
- ✓ Review each Award to determine if research involves the use of PHI or PII;
- ✓ Confirm IRB approval;
- ✓ Execute appropriate agreements; and
- ✓ Document Compliance with the Privacy Rule in the Award Backup.

ADDITIONAL RESOURCES

The screenshot shows a web browser window displaying the HHS.gov Health Information Privacy page. The browser's address bar shows the URL <https://www.hhs.gov/hipaa/>. The page features a blue header with the HHS.gov logo and the text "U.S. Department of Health & Human Services" and "Health Information Privacy". Below the header is a search bar with the placeholder text "I'm looking for..." and a magnifying glass icon. To the right of the search bar is a link for "HHS A-Z Index". Below the search bar are four navigation buttons: "HIPAA for Individuals", "Filing a Complaint", "HIPAA for Professionals", and "Newsroom". Below these buttons is a breadcrumb trail: "HHS Home > Health Information Privacy". To the right of the breadcrumb trail are options for "Text Resize" (with a font size of A A A), "Print", and "Share" (with icons for Facebook, Twitter, and a plus sign). Below the breadcrumb trail is the main heading "Health Information Privacy". Below the heading is a section with a search bar and two links: "> Your Rights under HIPAA" and "> Covered Entities and Business Associates". To the right of the search bar is an illustration of a woman with a speech bubble that says "If I can see my medical records, then I may feel more in control of my diabetes." Below the illustration is a dark grey box with the text "Your Health Information, Your Rights!" and a link that says "New videos and fact sheet explain your".

<https://www.hhs.gov/hipaa/>

A WORD ABOUT HIPAA COMPLIANCE IN PRACTICE



Coming Next ... Learn More: *HIPAA Compliance*

For more information please contact Research Administration via ORAF@northeastern.edu or 617-373-5600.

Thank you.