HIPAA & Research

UNC Privacy Office

June 17, 2021

THE UNIVERSITY
of NORTH CAROLINA
at CHAPEL HILL

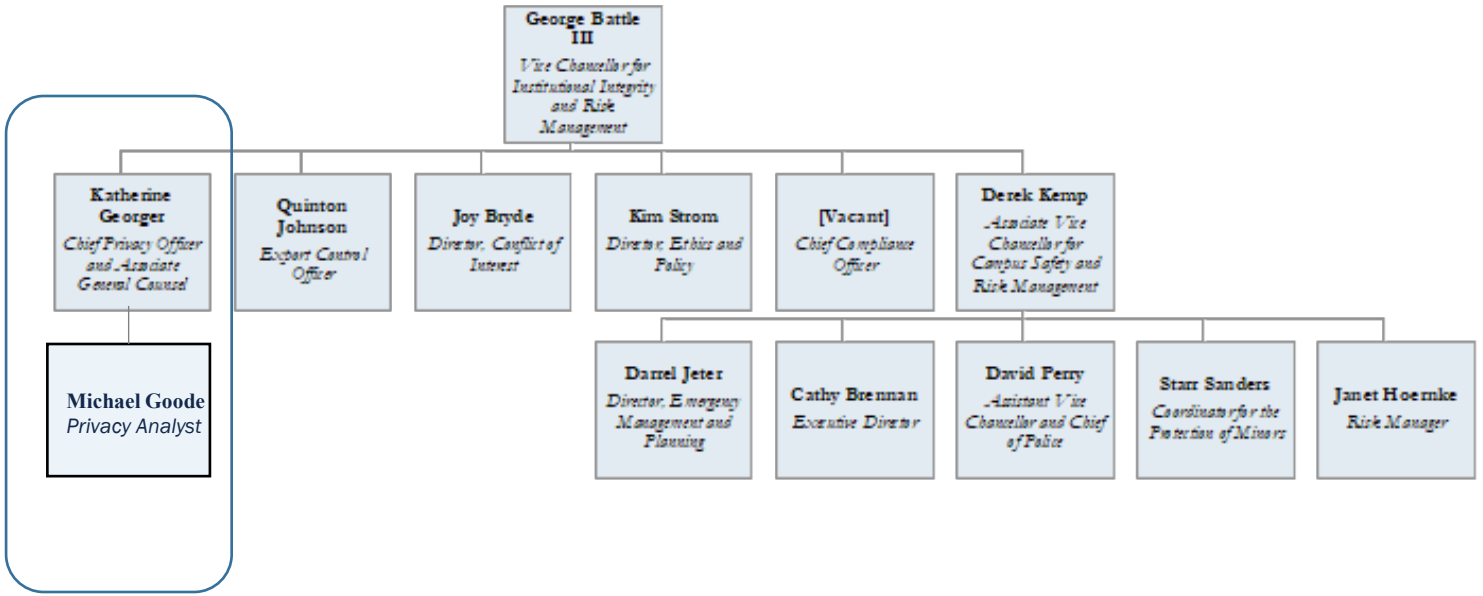
OBJECTIVES

- UNC Privacy Office
- HIPAA Overview
- HIPAA & Research
- Patient Rights & Research
- Privacy & Security Measures
- Privacy Incidents

UNC Privacy Office

UNC PRIVACY OFFICE

DIVISION OF INSTITUTIONAL INTEGRITY AND RISK MANAGEMENT
Organizational Chart
June 2021



UNC | INSTITUTIONAL INTEGRITY AND RISK MANAGEMENT

UNC PRIVACY OFFICE ACTIVITIES

- Federal and state laws and regulations govern different types of protected information and how that information may be used or disclosed and the IPO has responsibility across the entire University community on privacy-related matters implicating federal and state law including HIPAA.
- Advise University constituents on limiting the **use** (or sharing of information within an organization), **disclosure** (or sharing of information outside an organization), nature and amount of data (e.g., minimum necessary); implementing **reasonable safeguards** and **data management plans** to protect data.
- Develop and update **policies and procedures** to ensure compliance with applicable federal and state requirements.
- Review, revise and develop privacy statements, **privacy notices**, **authorizations**, user acknowledgments, attestations.
- Review, edit and negotiate data sharing **agreements** (data use agreements, data transfer agreements, material transfer and sometimes business associate agreements) with third parties or collaborators that may receive or transmit data.
- Investigate and respond to **privacy incidents** to determine if there has been an unauthorized acquisition, access, use or disclosure of research data that compromises the privacy and security of the data and requires reporting under applicable state or federal law.
- Prepare and implement **training** to University workforce members.

Seven Elements of an Effective Privacy Compliance Program

HIPAA Overview

WHO IS COVERED BY HIPAA?

- Health Care Providers: those that transmit health information in electronic form in connection with a covered transaction (engage in Standard Transactions under the HIPAA Transaction Standard)
- Health Plans: group health plans (employer sponsored health plans), HMOs, health insurance companies
- Health Care Clearinghouses: process or facilitate processing of health information into/from standard transactions
- Business Associates: creates, receives, maintains, transmits or stores PHI on behalf of a CE; provision of the service requires PHI to perform the job function; requires Business Associate Agreement

*The University of North Carolina Chapel Hill, like many academic medical centers, is a **hybrid entity**. The HIPAA Privacy Rule allows an organization to designate health care components, where the business activities of the health care components are "covered" functions subject to HIPAA, while non-health care component business activities are non-covered functions and not subject to HIPAA.

HIPAA: THE RULES

Privacy Rule

- Regulates what entities subject to HIPAA (including providers & business associates) must do to safeguard information;
- Identifies Protected Health information("PHI"); and
- Outlines individual's rights regarding their PHI (e.g., Notice of Privacy Practices, confidential communications, right of access, amendment, accounting)

Security Rule

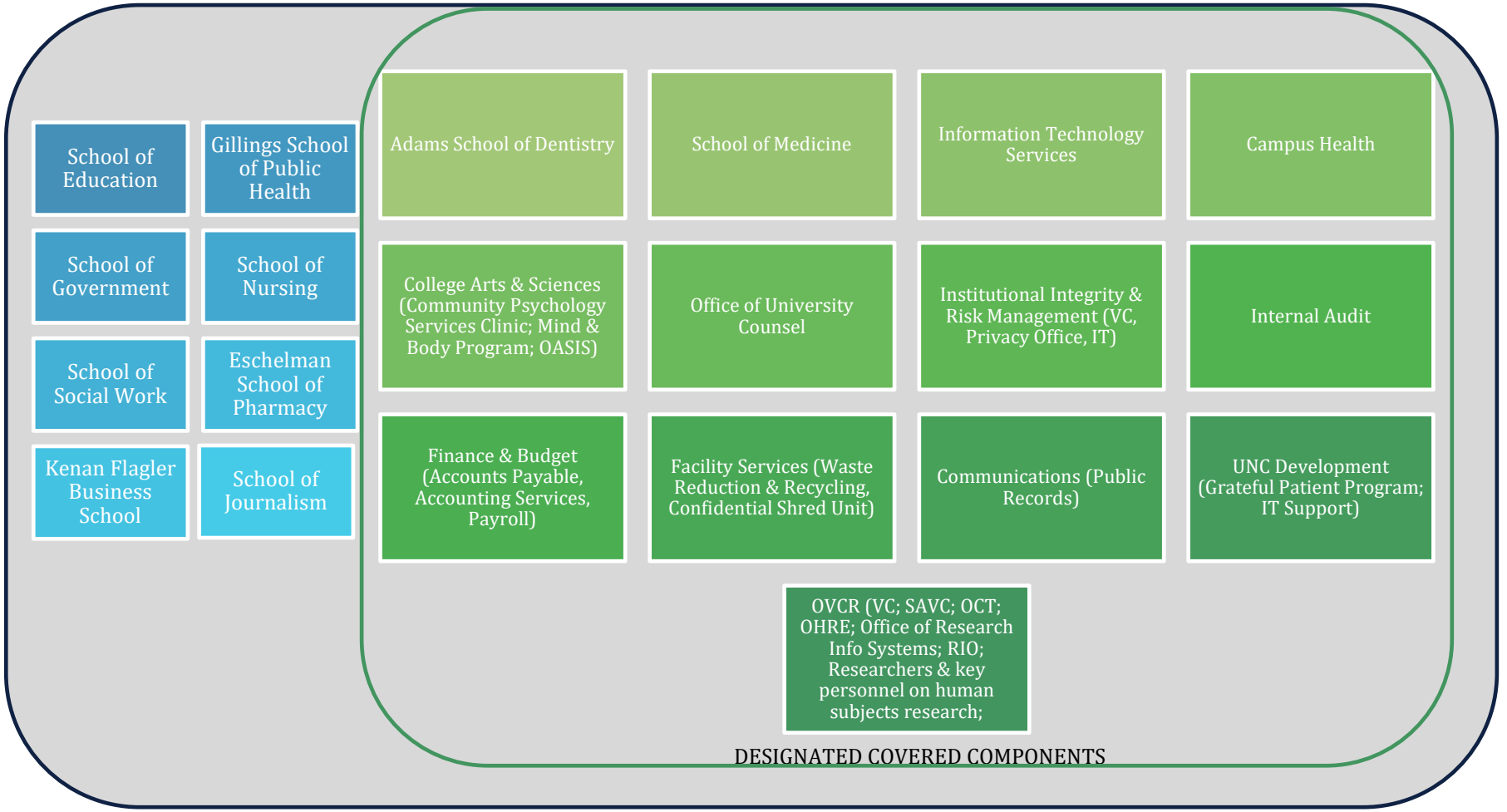
- Applies to electronic PHI ("ePHI")
- Regulates that organizations must ensure the availability, confidentiality and integrity of ePHI

Breach Notification Rule

- Requires written notice to affected individuals and the federal government (and the media if more than 500 affected individuals) if a breach of PHI occurs

**The HIPAA rules are enforced by the Office for Civil Rights (OCR), a division of the United States Department of Health & Human Services (HHS). Civil penalties range from $100 to $1.5 million per violation. There is also the potential for criminal penalties for knowingly or intentionally obtaining or disclosing PHI without patient authorization.

WHO IS COVERED BY HIPAA AT UNC: COVERED COMPONENTS



*Note: There are more units that fall outside of UNC's Covered Components that are not listed here. They have been omitted simply to better facilitate this illustration.

- UNC is a **Hybrid Entity** under HIPAA, which means that not all of UNC is covered by HIPAA.
- Only HIPAA **Covered Components** are subject to HIPAA including:
  - Unit that would meet the definition of a **covered entity** if it were a separate legal entity
  - Unit performs **covered functions** or transactions under HIPAA
  - Unit performs **business associate** functions
  - Extent a component uses PHI for **research** and/or **education** purposes.

WHAT IS PROTECTED?

Created or received by a health care provider, health plan or clearinghouse

+

Relates to past, present, future health condition, treatment, or payment of an individual

+

Identifies an individual (18 identifiers) OR Reasonable basis to believe could identify the individual

=

PHI

- PHI can be transmitted and stored in any medium or form, including: paper copies, verbal communications, video and audio recordings, digital images, other electronic formats.

Paper

Verbal

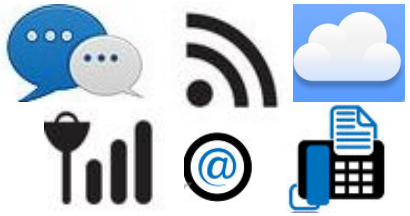
Video

Audio

Digital Images

Devices

Electronic Format



WHAT IS PROTECTED: HEALTH INFORMATION IDENTIFIERS

(1) Names.

(2) Geographic subdivisions smaller than a state (e.g., street address, city, county, etc.).

(3) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death, and all ages over 89.

(4) Telephone numbers.

(5) Fax numbers.

(6) Electronic mail addresses.

(7) Social Security numbers.

(8) Medical record numbers.

(9) Health plan beneficiary numbers.

(10) Account numbers.

(11) Certificate/license numbers.

(12) Vehicle identifiers and serial numbers, including license plate numbers.

(13) Device identifiers and serial numbers.

(14) Web URLs.

(15) Biometric identifiers, including finger or voice prints.

(16) Full face photographic images and any comparable images.

(17) Internet Protocol address numbers.

(18) **Any other unique identifying number characteristic or code.**

***** What constitutes "**any other unique identifying characteristic**"?

Anything that distinguishes an individual and allows for identification. For example, a unique identifying characteristic could be the occupation of a patient, for instance, "current President of State University"

Source: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html#supress

WHAT'S THE DIFFERENCE: PHI, LIMITED DATA SET, DE-IDENTIFIED DATA

Identifiable Data Sets

- PHI (18 HIPAA identifiers-data elements of the individual or relatives, employers or household members of the individual)
- Minimum Necessary Requirement (limit unnecessary or inappropriate access to and disclosure of PHI)
- Use/Disclose generally permitted for Treatment, Payment, and Health Care Operations

Limited Data Set

- Subset of PHI
- Limited use to (1) research, (2) public health activities OR (3) health care operations(QI)
- Data set stripped of certain direct identifiers specified in the Privacy Rule
- Leaves dates (e.g., Date of Birth, Dates of Service) and certain geolocation data (city, state, county, zip code)
- Requires Data Use Agreement (DUA required before any use/disclosure of LDS to third-party)

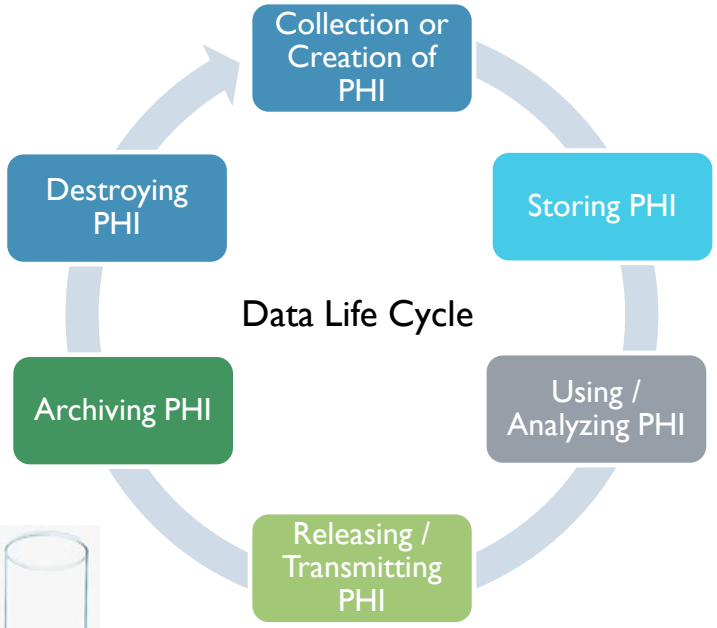
De-Identified Data

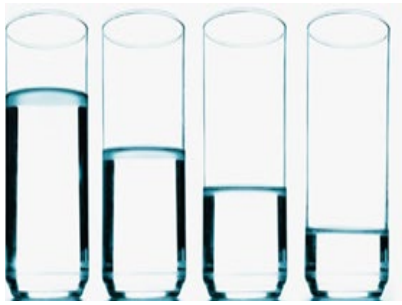
- Data set is stripped of all 18 identifiers (***Safe Harbor Method***) OR is de-identified by the ***Expert Determination*** method (certification from qualified statistician that risk of re-identification of individual is low)
- https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/
- No longer considered PHI under HIPAA
- Obligated not to re-identify
- Duke Health requires safeguarding such datasets

HIPAA & RESEARCH

OVERVIEW: HOW DOES HIPAA IMPACT RESEARCH?

- HIPAA regulations govern who is covered, what type of information is covered and how that information may be used, including:
  - Limiting the **use** (or sharing of information within an organization) and **disclosure** (or sharing of information outside an organization) to the **minimum necessary** (need to know basis based on job-specific function and purpose).
    - General requirement to obtain **individual authorization** for such things as marketing, sale of PHI, research; however, certain exceptions including **treatment, payment** and **health care operations** and waiver of authorization by IRB.
  - Individual rights (right to **access**, right to request **amendment**, right to **accounting of disclosures**)—obligation for an accounting where no patient authorization obtained
    - **Notice of privacy practices**—describes how an organization will use and protect an individual's PHI and the patient's rights)--should include language about how patient's information may be used for research purposes.
  - Adopting **reasonable safeguards** to protect PHI data during the entire **data lifecycle** (e.g., physical locking PHI during non-business hours; securing workstation; encrypted laptops and mobile devices; shredding documents)
  - Executing **business associate agreements** with third parties that create, receive, transmit, maintain or store PHI on behalf of the University's Covered Entity components (e.g., storage vendor) or **data use agreements** with third parties that may receive or transmit a limited data set.
  - Reporting and investigating any **privacy incident** to determine if there has been an unauthorized acquisition, access, use or disclosure of PHI that compromises the privacy and security of the data.





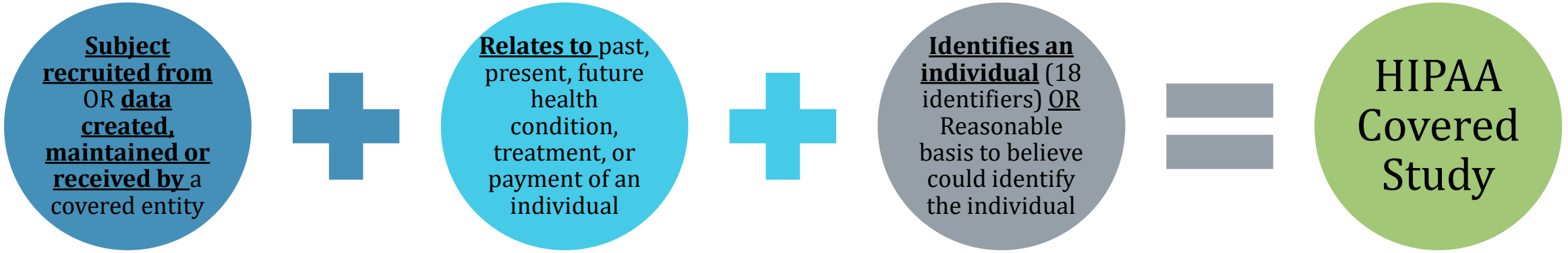
Minimum Necessary

Business Associate Agreements & Data Use Agreements

RESEARCH: HIPAA COVERED STUDIES

At UNC, research would be considered to involve PHI and thus be subject to HIPAA if **all** of the following conditions are met:

- The subject is recruited from AND/OR data is created, maintained or received by UNC Health, a UNC Covered Component, or any other covered entity; AND
- The data relates to health information; AND
- The data includes any of the 18 HIPAA identifiers.



RESEARCH: APPLICATION OF HIPAA

HIPAA Privacy Rule Applies

The HIPAA Privacy Rule applies to the following types of research activities when they involve PHI:

1. Research using or creating PHI about living individuals
2. Activities preparatory to research
3. Research on decedents who have been deceased 50 years or less
4. Recruitment
5. Research using a limited data set

HIPAA Privacy Rule Does NOT Apply

The types of research that do **not** fall under the HIPAA Privacy Rule are:

1. Research using de-identified data
2. Research conducted by an individual who is not part of a covered entity and that does not require access to information held by a HIPAA covered entity
3. Research on individuals who have been deceased more than 50 years

RESEARCH: USING OR CREATING PHI OF LIVING INDIVIDUALS

PHI may not be used for research purposes unless at least one of the following conditions applies:

- Consent or Waivers of Informed Consent Obtained Prior to April 14, 2003
- Subject Authorization For Research
- IRB Approved Waiver of Authorization
- The study involves only de-identified data or a limited data set

HIPAA AUTHORIZATION FOR RESEARCH PURPOSES

- HIPAA generally requires a written authorization from the subject permitting a researcher to use or disclose the subject's PHI for research purposes. The researcher is required to get written authorization from the research participant or the personal representative of the participant.
- Under HIPAA the Research Authorization Form (RAF) can be combined with the Informed Consent Form (ICF) for the same study, called a Compound Authorization.
- At UNC, the current practice is to have a separate HIPAA Authorization and ICF.
- Core HIPAA Authorization Requirements:
  - A specific description of what PHI will be used/disclosed.
  - The names of persons or organizations who may use or disclose PHI.
  - The names of persons or organizations to whom PHI will be disclosed.
  - A statement of the purpose of the use/disclosure.
  - A statement of how long the use or disclosure will continue (no expiration date is permitted for research purposes; however, this must be specifically stated in the authorization form and justification must be noted in the protocol).
  - A statement that the authorization may be revoked.
  - A statement regarding the potential for re-disclosure of information to others that is not subject to the Privacy Rule.
  - A notice that the covered entity may not condition treatment or payment on the individual's signature absent certain exceptions.
  - The individual's signature and date.
- A copy of the signed authorization must be provided to the individual
- Disclosures of PHI made in connection with research conducted pursuant to signed authorization **do not** need to be tracked for purposes of responding to an individual who requests an **accounting of disclosures**
- Copies of the signed authorization and the Request Access to PHI for Research Purposes form should be provided to the record holder to obtain access to the appropriate records, where feasible. Otherwise, the form should be stored with the research records for at least 6 years

WAIVER OF AUTHORIZATION

- A waiver of authorization is permitted only when the following conditions exist:
  - The research could not be practicably conducted without the waiver.
  - The research could not be practicably conducted without access to and use of PHI.
  - A written assurance to the IRB that the PHI will not be re-used or disclosed except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of protected health information would be permitted by the Privacy Rule.
  - Uses and disclosures of PHI will be limited to the minimum necessary standard.
  - Disclosure involves no more than minimal privacy risk to the individuals.
  - Reviewed by the IRB with specific approval regarding access to the PHI.
- Waiver applications must describe plan for protecting identifiers, destroy identifiers as quickly as possible, and tracking disclosures.
- The criteria for waiver are very similar to those for waiving informed consent. This means that if a research plan includes obtaining informed consent from research participants, it is not likely that a waiver of HIPAA authorization will be granted, except perhaps for recruitment purposes.
- Accounting of Disclosures Policy. Disclosures of PHI that are made in connection with research conducted pursuant to a Waiver of HIPAA Authorization must be tracked in order to respond to individuals who request an accounting of disclosures of their PHI. *It is the responsibility of investigators to track such disclosures made in connection with their own research protocols.*

ACTIVITIES PREPARATORY TO RESEARCH

- PHI may be accessed in activities that are "preparatory to research." This type of access is limited to a review of data to assist in formulating a hypothesis, determining the feasibility of conducting the study, determining cell size, or other similar uses that precede the development of an actual protocol.
- While an investigator may review PHI during the course of a review preparatory to research, he or she may not remove, copy or include any PHI in notes. Summary data (e.g., count of individuals with a certain disease) may be written down and removed.
- PHI may not be used to identify potential research subjects by name or by any other identifier under HIPAA.

RESEARCH ON DECEDENTS

- HIPAA requires that researchers who wish to access PHI of decedents who have been deceased 50 years or less first make certain representations to the holder of the PHI.
- The researcher must represent that:
  - The use or disclosure of PHI is solely for research on the PHI of decedents.
    - This means the researcher may not use the PHI of the decedent to obtain information about a decedent's living relative(s).
    - A researcher may request a decedent's medical history for an outcome study relating to treatment previously administered to the decedent.
  - The researcher must also provide written assurances that the PHI is necessary for the research.
  - The holder of the PHI has a right to require documentation of death of the individuals about whom information is being sought.
- The health information for individuals who have been deceased for more than 50 years is not subject to the HIPAA requirements.

RECRUITMENT

- Under HIPAA, the use of PHI to recruit an individual to participate in a research study must comply with HIPAA's general requirement that the use must be pursuant to an authorization or some exception, such as a **partial waiver** of HIPAA Authorization.
- Although recruitment procedures usually only require access to a limited amount of health information, recruitment nonetheless is considered to be accessing PHI and therefore must comply with HIPAA requirements.
- Researchers are required to obtain a subject's authorization after recruiting and enrolling subjects via a partial waiver and prior to creating or using PHI during research procedures.
- A **treating provider** may:
  - Discuss with his/her own patients the option of enrolling in a study.
  - Obtain written authorization from the patient for referral into a research study.
  - Provide research information to the patient so that the patient can initiate contact with the researcher.
  - Provide the information to a researcher when the researcher has obtained an approved Waiver of Authorization from an IRB for recruitment purposes.

LIMITED DATA SET

- HIPAA permits use of a “limited data set” for research purposes.
- A limited data set is PHI that excludes “direct identifiers” of the individual, relatives of the individual, employers, or household members.
- Leaves dates (e.g., date of birth, death, service), certain geolocation data (city, state, county, zip code (less than 20,000 citizens)) and other unique identifying numbers, characteristics, or codes not expressly excluded (MRN, accession numbers are excluded).
- A limited data set must be used for one of the following purposes: (1) research, (2) public health activities OR (3) health care operations(QI)
- Requires Data Use Agreement (DUA required before any use/disclosure of LDS to third-party)
  - Establishes permitted uses and disclosures of the information included in the limited data set and must provide that the recipient of the limited data set will not re-identify the information or use it to contact individuals
- Like research pursuant to an authorization, disclosures of LDS do not need to be tracked for accounting of disclosures purposes.

EXEMPT STUDIES

- Studies Exempted from IRB Review Studies which have been exempted under the Common Rule but which involve the use of PHI are not also exempted under HIPAA.
- HIPAA requirements related to authorization or waiver are applicable to these studies.
- Investigators should provide a HIPAA Research Authorization Form or Request for Waiver of HIPAA Authorization to the IRB along with the exemption request.

Patient Rights & Research

NOTICE OF PRIVACY PRACTICES RESEARCH EXAMPLES

UNCH Notice of Privacy Practices

We may use and/or disclose your PHI in a number of circumstances for which we need not seek your permission or give you an opportunity to agree or object, such as:

****

For research or to collect information in databases to be used later for research. We may disclose your PHI, and surplus specimens, for research that is approved by an institutional review board that has determined that your written consent to the disclosure is not required. We may also review your PHI to determine if you are eligible to participate in a medical research study or to allow a researcher to contact you via phone, email, text message or by mail to determine if you are interested in participating in a medical research study.

Duke Health Notice of Privacy Practices

Research. Under certain circumstances, we may use and disclose health information about you for research purposes. For example, we may use health information in preparing to conduct a research project or to see if you are eligible to participate in certain research activities. Before we use or disclose health information for research, however, the research project will have been approved through a specialized approval process. We may also contact you to see if you are interested in participating in research. If you do not wish to be contacted to participate in research, please contact Research Navigators at 919-660-9172 or myresearchnavigators@duke.edu. We will use reasonable efforts to prevent this research contact. Calling Research Navigators will not apply to the use of your health information for research purposes as described above and will not prevent your providers from discussing research with you.

RIGHT OF ACCESS

- Under HIPAA, a patient has a right to access their PHI that is maintained in the patient's designated record set. This may include PHI generated during the course of a research study if that research information is stored in the patient's designated record set. The designated record set includes any health information which was used to make a treatment decision (patient's legal medical record).
- Investigators or departments conducting research in conjunction with treatment are given the option to determine whether research notes which are collected purely for research purposes are included into the designated record set.
- However, data collected during a research study, which is used for treatment decisions, would be included in the DSR.
- Researchers can deny subject access to information contained in the research record or delay granting access until after the study is complete. If access is to be restricted for the course of the study, this restriction must be indicated in the HIPAA research authorization form. Upon completion of the study, participants may request and be provided with a copy of their records.

ACCOUNTING FOR DISCLOSURES

- HIPAA requires that, upon request, patients be provided with a listing of individuals external to the HIPAA covered entity who have had access to or been provided a copy of their records for reasons other than treatment, payment, healthcare operations or with the patient's authorization.
- In the context of research at UNC, researchers have the responsibility of maintaining accounting logs for any disclosures to a third party (including an individual not part of UNCH or the UNC covered components) where prior authorization has not been obtained (i.e., waiver of authorization). These logs can be maintained with the records or in an electronic database.
- Research records themselves are also subject to the accounting requirement when study PHI is:
  - Accessed for secondary data analysis by another researcher outside the UNC covered components
  - Accessed by additional researchers or entities not included in the authorization form signed by the subject or
  - Disclosed in unanticipated events such as theft or loss of records.

ACCOUNTING FOR DISCLOSURES

- UNC Health Policy provides:
- IRB Approved Research and the Obligation of the Researcher for Tracking Disclosures for Research Purposes.

  a. Any individual performing research approved by the UNC Institutional Review Board (IRB) must track disclosures to third parties of any PHI received from a UNCHCS Facility that is disclosed to a third party for which a prior authorization from the subject has not been received (typically in the event a waiver of authorization has been issued by the IRB).

  b. In the event the individual researcher discloses PHI for a particular research purpose for fifty (50) or more individuals, the accounting may, with respect to such disclosures for which the PHI about the individual may have been included, provide an aggregated description of data disclosed as follows:

    i. The Name of the protocol or other research activity;

    ii. A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;

    iii. A brief description of the type of PHI disclosed;

    iv. The date, or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;

    v. The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and

    vi. A statement that the PHI of the individual may or may not have been disclosed for a particular protocol or other research activity.

RECORDS RETENTION

- HIPAA related documentation must be maintained for six (6) years. This requirement applies to accounting for disclosures records, authorizations, data use agreements and any other HIPAA forms.
- In accordance with Minimum Necessary requirements, the data itself should be de-identified as soon as possible following the completion of the study.
- If the retention of identified data is contemplated, such retention must be justified and approved by the IRB, including plans for securing the data.

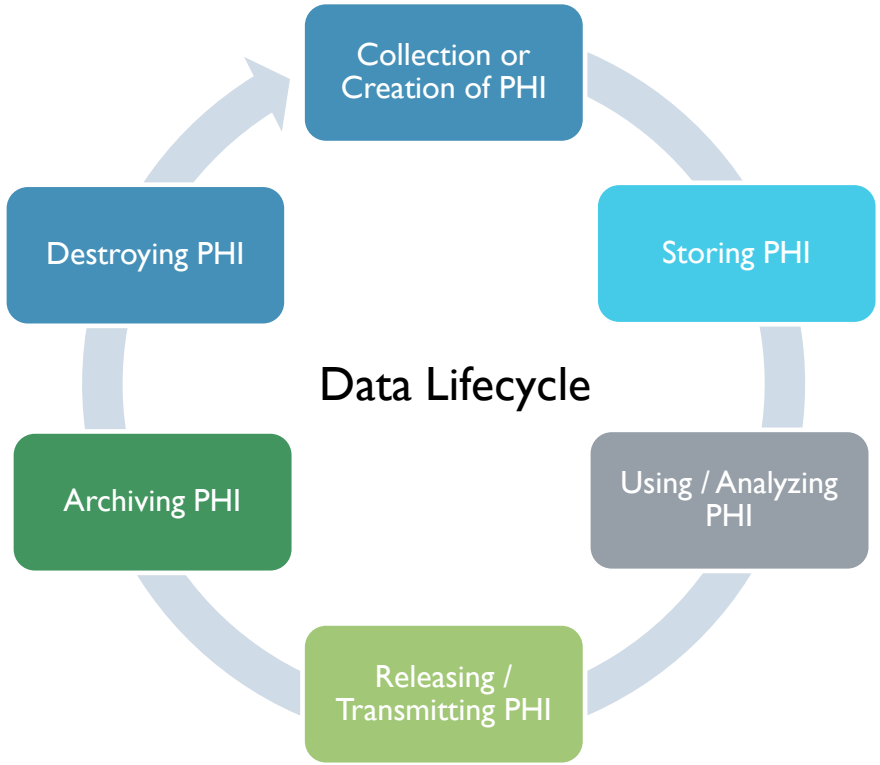
Privacy & Security Measures

SAFEGUARDING PHI

- In order to prevent incidents from occurring, it is critical that when performing your job and handling PHI that you properly safeguard PHI at all times. Here are some simple steps you can take to safeguard PHI:
  - Whenever possible, keep conversations about subjects or involving subjects private and speak softly when in a non-private setting so that the conversation may not be overheard by others nearby;
  - Do not use patient/subject names in public areas such the cafeteria, hallways, and elevators;
  - Reduce the visibility of hard copy records and other documents containing PHI by, for example, turning documents over, covering them, or placing them in a file when not in use and locking them in a drawer at night;
  - Use privacy screens for your PC and/or laptop;
  - Avoid leaving subject records with PHI unattended or cover them if possible;
  - Make sure that all PHI is disposed of properly (e.g., locked bin or shredder or if electronic, securely disposed);
  - Promptly remove all documents from fax machines, copy machines, and printers;
  - Protect your passwords and do not share them with anyone; and
  - If you will be storing sensitive information on your desktop/laptop or thumb drive, ask your IT personnel about options to encrypt your device or to talk to them about other storage solutions available to UNC workforce members.
- If you see any PHI that appears to be inappropriately safeguarded, bring this to the attention of UNC Privacy Office (privacy@unc.edu)

YOUR RESPONSIBILITY TO PROTECT PHI THROUGHOUT THE DATA LIFECYCLE

- You are responsible for adopting **reasonable safeguards** to protect PHI data during the entire **data lifecycle**
  - Paper PHI:
    - Collection/creation—only the minimum necessary
    - Storage—physically locking PHI during non-business hours
    - Transmission—de-identify (where possible), don't leave items unattended or in cars, consider locking bags
    - Destruction—locked bins, shredders.
  - ePHI:
    - Collection/creation—only the minimum necessary
    - Storage—secure workstations, encrypted laptops/mobile devices, UA approve solutions (REDCap, UNC Office 365)
    - Transmission—de-identify (where possible); encrypted in transmission and at rest ("end to end encryption")
    - Destruction—talk with ITS or your local IT personnel when "wiping" devices (you may think it is wiped, but there could be cached files). Encryption is the gold standard.



IRB PROTOCOLS: RESEARCH DATA MANAGEMENT

In their IRBIS application, researchers MUST:

1. Specify the Protected Health Information (PHI) or other individually identifiable data or specimens the researcher will obtain, use or disclose to others—be specific (ask for specific data elements (e.g., full name, MRN, SSN, DOB, device serial #))
2. Comply with University Policy that requires that ALL electronic devices that may hold identifiable participant data will be secure (e.g., password protected, backed up, and/or encrypted)
3. Provide any additional information on ALL data privacy and security measures taken (e.g., if paper PHI locked, location of keys, who has access to keys; if ePHI, ask if local drive, UNC servers, UNCH laptop, UNC-issued laptop, password protected, encrypted)
4. Indicate who will have access to identifiable data, including researchers, collaborators, consultants

IF researcher indicates that he/she will be using Protected Health Information (PHI) and at least one of the following is contained in the application:

- *Intent to develop, adopt, employ, implement* new technology or platform (i.e., database, repository, software, hardware, app);
- *Intent to use* third-party vendor's platform (i.e., Cloud computing, processing or storage) as part of the project,
- *Intent to collaborate*, *coordinate*, or *use* the services, including software or hardware, of outside consultants, collaborators and/or third parties

THEN these are often RED FLAGS that a more comprehensive security and privacy review needs to be conducted to ensure the integrity of UNC Sensitive Information is adequately safeguarded.

**NOTE: Currently, ITS Security Reviews are ONLY triggered if researchers submit a requisition with Purchasing that triggers a DPC.*

UNENCRYPTED COMMUNICATIONS

HIPAA Security Rule:

- Standard: Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. 45 CFR § 164.312(e)(1).
- "Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information." 45 CFR § 164.312(e)(2)(ii).
- "[C]overed entities are permitted to send individuals unencrypted emails if they have advised the individual of the risk, and the individual covered entity to notify the individual that there may be some level of risk that the information in the email could be read by a third party….If individuals are notified of the risks and still prefer unencrypted email, the individual has the right to receive protected health information in that way, and covered entities are not responsible for unauthorized access of protected health information while in transmission to the individual based on the individual's request. Further, covered entities are not responsible for safeguarding information once delivered to the individual." 78 Fed. Reg. 5634 (Jan. 25, 2013).

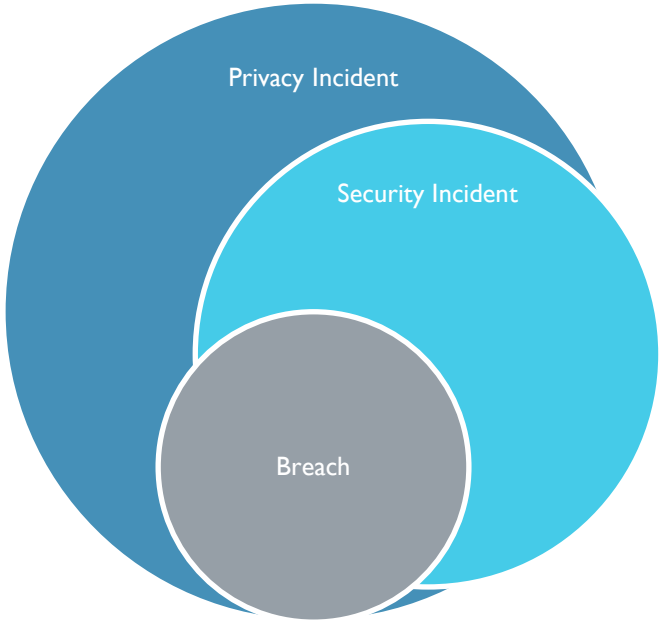
UNC Policy and Procedure:

- As of 10/26/2020 the "Transmission of Sensitive Information" standard has been updated. This standard details the use of unencrypted communication.
- If your study is utilizing unencrypted communications, properly complete section A.4.6 in IRBIS.
- Common questions and answers regarding the use of unencrypted communications can be found here: Unencrypted Communication - UNC Research

Privacy Incidents

PRIVACY INCIDENT

- **Privacy Incident**: any loss of control, compromise, or unauthorized disclosure, acquisition, access of *protected health information* (PHI), whether physical or electronic.
- **Security Incident**: any attempt, successful or unsuccessful, to access, use, disclose, modify or destroy ePHI or interfere with protective system controls.
- Key Incident Characteristics:
    1. Unauthorized persons
    2. Unauthorized purpose
    3. Includes both successful efforts and unsuccessful attempts
    4. Intent not required
- **Breach**: any *successful* compromise of protective controls, or **unauthorized acquisition, disclosure**, **access or use of** PHI not permitted by HIPAA which **compromises** the security or privacy of PHI **and** which triggers a reporting obligation by state/federal law to those affected individuals.



PRIVACY INCIDENT PROCESS

Report: IMMEDIATELY notify the UNC Privacy Office whenever an incident is suspected—even seemingly minor or innocuous incidents. privacy@unc.edu

Detailed Summary: Provide a clear & concise description of the incident, including any relevant documents or information related to the incident; cooperate with the Privacy Office's investigation.

Mitigation: If you took any mitigation efforts, please describe what your office did to mitigate the incident to prevent further unauthorized access, use or disclosures; Privacy Office may assist you in your mitigation efforts.

Corrective Action Plan: Explain what corrective actions your office took to prevent future incidents; Privacy Office may assist you in identifying corrective measures.

Notification: If Privacy Office determines an incident rose to level of a reportable breach, Privacy Office will draft notification letters, with your office's assistance.

INCIDENT REPORTING AND NSI POLICIES

- If a privacy incident occurs, or is suspected, IMMEDIATELY notify the UNC Privacy Office (privacy@unc.edu) regardless of whether the incident appears minor or innocuous. The Privacy Office has an independent obligation to assess whether the incident is reportable under applicable or federal state data privacy law.
  - Incidents trigger potential time-sensitive deadlines under certain federal and state laws so it is imperative that any incident, or potential incident, is reported to the Privacy Office as soon as possible to allow for sufficient time for investigation.
- As previously discussed, if the Privacy Office determines an incident rose to level of a reportable breach, the Privacy Office will draft notification letters.
- Additionally, be aware of all UNC Policies and Procedures related to NSIs. (e.g., OHRE SOP 1401; 1402).
- "Information previously unknown to the IRB that suggests new or increased risk to subjects or others (hereinafter referred to as New Safety Information) is promptly reportable to OHRE **within 7 calendar days** of the investigator becoming aware of the information. "
  - This includes any breach **or potential breach** of subject privacy.

ACADEMIC MEDICAL CENTERS/UNIVERSITY BREACHES IN THE NEWS…

- **University of Texas MD Anderson Cancer Center (stolen or lost unencrypted devices with ePHI of over 33,500 subjects)*** MD Anderson claimed it was not obligated to encrypt its devices because ePHI was for research, and was not subject to HIPAA. An Administrative Law Judge (ALJ) rejected this argument. **$4.3 million** (6/18/2018)
- **UMass Amherst (malware infected workstation impacted1,670 individuals)** UMass failed to designate all of its Health Care Components when hybridizing, incorrectly determining that SLH Center where the breach of ePHI occurred, were not covered components. **$650,000** (11/22/2017)
- **Mississippi Medical Center** (**password protected computer stolen from ICU 10,000 individuals**) OCR found that UMMC was aware of risks & vulnerabilities dating back to 2005, but no significant risk management activity occurred until after breach. **$2.75 million** (7/25/2016)
- **Oregon Health & Science University (unencrypted laptop (4,022) , unencrypted thumb drive or cloud (3,044))** Found widespread vulnerabilities in HIPAA compliance program. Students/residents used unencrypted thumb drives or cloud-based solution without a BAA. Plus 2 large breaches 2009 & 2012 (unencrypted laptop, unencrypted thumb drive impacting 15,000 patients). **$2.7 million** (7/18/2016)
- **University of Washington Medicine** Failure to implement policies to prevent, detect, contain, and correct security violations. Employee downloaded email containing malware – affecting 90,000 individuals/patients who had their ePHI accessed. Underscores need for organization-wide risk analysis. **$750,000** (12/14/2015)
- **New York Presbyterian/Columbia University (disclosure of ePHI of 6,800).** NYP & CU are separate covered entities participating in an affiliation **$4.8 million** (5/7/2014) Two years later, NYP paid another $2.2 million (4/21/2016) for the unauthorized filming of two patients.

HIPAA & RESEARCH: SIMILAR PRINCIPLES

Risks of a data breach in clinical settings are analogous to risks of a data breach within research settings:

- Human subjects research concerned with **confidentiality risks** associated with the research right to be free from unauthorized release of information that the individual has disclosed in a relationship of trust, with the expectation that it will not be disclosed to others without permission.
- The HIPAA Privacy Rule is broadly concerned with the risk to the subject's privacy associated with the **use and disclosure of the subject's PHI**. Understanding between participant and investigator (as set forth in the consent and authorization documents) as to how participant information will be handled, managed and disclosed to others as part of the research.
  - **Respect for persons**—researchers actively protect privacy (HIPAA authorizations or waivers of authorization) and use appropriate privacy and security measures (data security safeguards) to avoid breaching participant confidentiality.
  - **Beneficence**—use of private information justified by benefit of research and minimizing harm from research, including invasion of privacy and confidentiality
  - **Justice**—balance description of risks to subject confidentiality with the measures you will take to prevent harm (minimum necessary, agreements, security management plans, encrypted devices, reporting incidents)

HIPAA ENFORCEMENT & RESEARCH

- OCR Director Jocelyn Samuels offered this cautionary warning:

  "Research institutions subject to HIPAA must be held to the same compliance standards as all other HIPAA-covered entities…**For individuals to trust in the research process and for patients to trust in those institutions, they must have some assurance that their information is kept private and secure.**"

  OCR Press Release, March 17. 2016

  http://www.hhs.gov/about/news/2016/03/17/improper-disclosure-research-participants-protected-health-information-results-in-hipaa-settlement.html

COSTS OF A BREACH

- **Financial.** There are financial costs to UNC and to the affected individuals associated with privacy breaches. UNC may have to pay millions of dollars in regulatory fines and litigation related costs. Additionally, affected individuals may pay a heavy price for restoring their credit and identity in the event they are a victim of financial fraud and/or identity theft.
- **Emotional.** There is also a human cost associated with a privacy breach. A privacy breach can be emotionally devastating to individuals who are the victims of identity theft or other financial fraud and as a result, affected individuals may suffer real emotional harm.
- **Reputation.** A privacy breach could also be devastating to the reputation of the University and its ability to attract research grants, awards and research participants.
- **Discipline**. A workforce member responsible for a breach may be subject to discipline up to and including termination of employment. Employees may also be individually liable (civil and criminal) for certain violations.

Questions?

UNC Privacy Office

Email: privacy@unc.edu

Phone: 919.962.6332

Visit: privacy.unc.edu

THE UNIVERSITY
of NORTH CAROLINA
at CHAPEL HILL