# Health Insurance Portability and Accountability Act (HIPAA)

## HIPAA Privacy & Security Considerations

## Student Orientation

The information in this presentation is designed to provide an overview of the HIPAA Privacy and Security regulations to comply with UB's student training obligations within its Student Affiliation Agreements. UB students participating in educational experiences within HIPAA covered entities should also receive HIPAA training from those entities specific to their activities as mandated by HIPAA. The presentation also addresses HIPAA in the context of UB research conducted within facilities required to comply with HIPAA

While reasonable efforts have been made to incorporate current, complete, and accurate information, UB does not guarantee or warrant that the information is current, complete, or accurate. The information contained in this presentation is subject to change at any time without notice. Last revised 8/10/2012.

# Target audience

UB students, faculty, and staff interested in a general overview of the Health Insurance Portability and Accountability Act (HIPAA) as it relates to the privacy and security of patient information and UB student training or research activities

The goal of the presentation is to provide a general introduction to some of the key concepts in HIPAA to help ensure that participants can proactively avoid taking actions that might create HIPAA violations for entities regulated by HIPAA

# Additional Training REQUIRED

HIPAA regulated entities must provide individuals working or training within them with HIPAA training that is specific to the entity's HIPAA policies and procedures. This presentation is intended to provide a context for that mandated training; it is not a substitute for that training

If you are a student or UB employee working with such a site and have not received this additional training, inquire as to how you can obtain it from your instructor or the entity's HIPAA officials

# Goals / Learning Objectives

- Understand HIPAA's origin
- Understand who HIPAA applies to and its role in protecting the confidentiality, integrity and availability of patient information
- Understand key elements of the HIPAA Privacy and Security rules related to student training and research
- Understand the penalties associated with HIPAA violations
- Understand how entities subject to HIPAA must respond to HIPAA violations

# Goals / Learning Objectives

- Understand data release mechanisms that permit the disclosure of protected health information from HIPAA regulated entities in both the student training and research contexts
- Understand the IRB's role in reviewing release mechanisms used at UB to acquire research data
- Familiarity with the following terms/concepts:

# Part – I
# HIPAA Origins

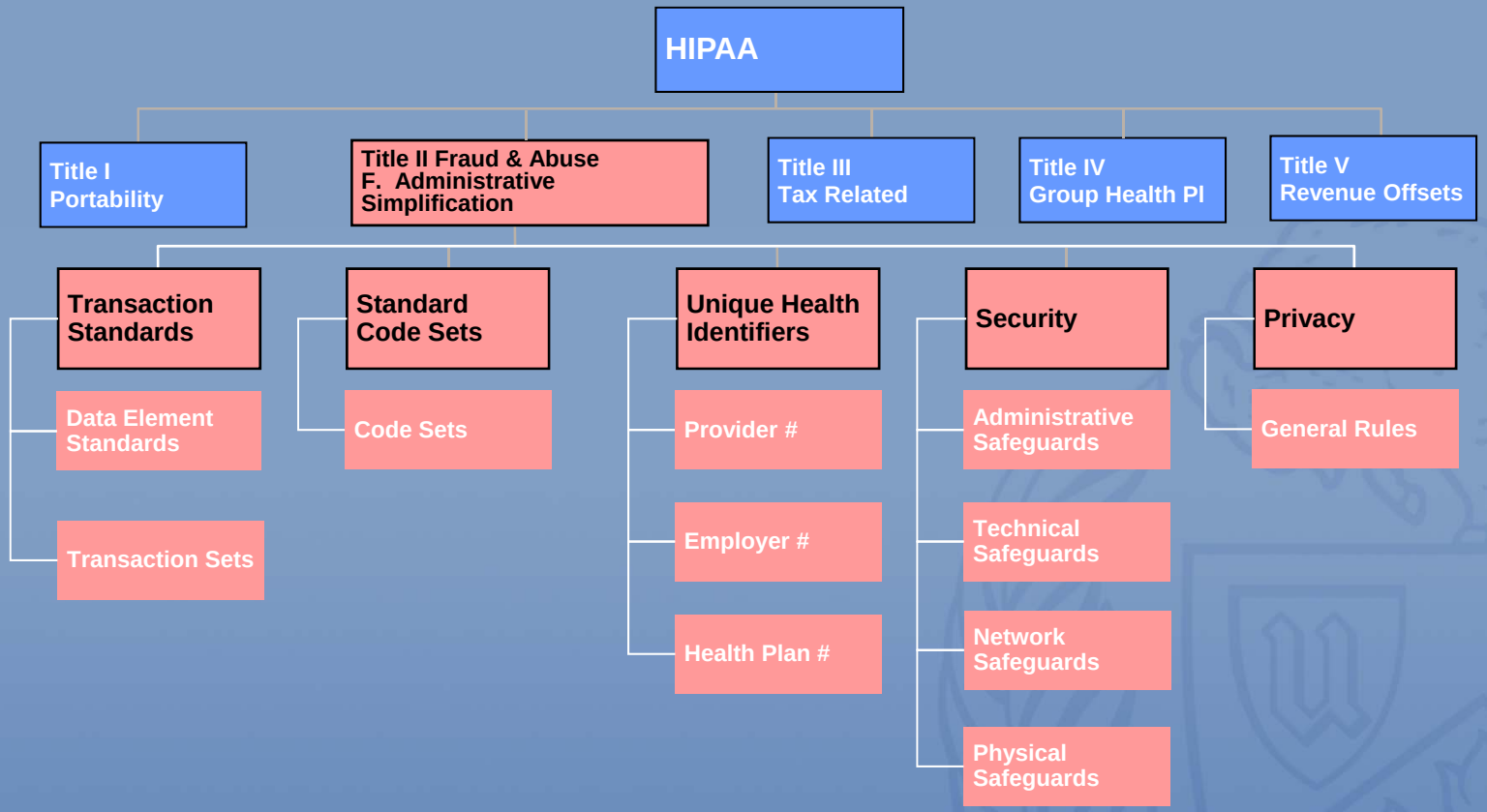
# What is HIPAA?

Public Law 104-191 (104th Congress); Aug. 21 1996

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

"An Act To amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes."

# The HIPAA law has many parts. For this orientation (and in common usage) HIPAA means the separate Privacy and Security standards within "Title II Fraud & Abuse"



# HIPAA regulations

The HIPAA law delegated development and promulgation of regulations associated with the law to the Secretary of Health and Human Services (HHS)

The resulting HHS regulations have many parts which can be found in the Code of Federal Regulations (CFR) Title 45 Public Welfare, Parts 160, 162 and 164.

# 45 CFR Part 160

## PART 160—GENERAL ADMINISTRATIVE REQUIREMENTS

- Subpart A—General Provisions ( § 101-104)
- Subpart B—Preemption of State Law ( § 201-205)
- Subpart C—Compliance and Investigations ( § 300-316)
- Subpart D—Imposition of Civil Money Penalties ( § 400-426)
- Subpart E—Procedures for Hearings ( § 500-552)

# 45 CFR Part 162

## PART 162—ADMINISTRATIVE REQUIREMENTS

- Subpart A—General Provisions ( § 100-103)
- Subparts B-C [Reserved]
- Subpart D—Standard Unique Health Identifier for Health Care Providers ( § 402-414)
- Subpart E [Reserved]
- Subpart F—Standard Unique Employer Identifier ( § 600-610)
- Subparts G-H [Reserved]
- Subpart I—General Provisions for Transactions ( § 900-940)
- Subpart J—Code Sets ( § 1000-1011)

# 45 CFR Part 162

- Subpart K—Health Care Claims or Equivalent Encounter Information ( § 1101-1102)
- Subpart L—Eligibility for a Health Plan ( § 1201-1202)
- Subpart M—Referral Certification and Authorization ( § 1301-1302)
- Subpart N—Health Care Claim Status ( § 1401-1402)
- Subpart O—Enrollment and Disenrollment in a Health Plan ( § 1501-1502)
- Subpart P—Health Care Payment and Remittance Advice ( § 1601-1602)
- Subpart Q—Health Plan Premium Payments ( § 1701-1702)
- Subpart R—Coordination of Benefits ( § 1801-1802)
- Subpart S—Medicaid Pharmacy Subrogation ( § 1901-1902)

# 45 CFR Part 164

## PART 164—SECURITY AND PRIVACY

- Subpart A—General Provisions ( § 102-106)
- Subpart B [Reserved]
- Subpart C—Security Standards for the Protection of Electronic Protected Health Information ( § 302-318)
- Subpart D—Notification in the Case of Breach of Unsecured Protected Health Information ( § 400-414)
- Subpart E—Privacy of Individually Identifiable Health Information ( § 500-534)

# HIPAA is intertwined & evolving

In 2009 another law was passed by Congress known as "The American Recovery and Reinvestment Act of 2009" (ARRA). Within this law was a section known as HITECH (TITLE XIII—HEALTH INFORMATION TECHNOLOGY SEC. 13001 Health Information Technology for Economic and Clinical Health Act)

HITECH among other things, made some changes to HIPAA such as mandating breach reporting, changing the HIPAA civil monetary penalty structure, and extending HIPAA compliance requirements and penalties to Business Associates of HIPAA regulated entities by law

# HIPAA and State Law

HIPAA is designed to establish a floor of minimum safeguards that must be met. Built into HIPAA is the concept of pre-emption analysis. If a state law is more protective ("stringent") then it preempts HIPAA in such cases. If a state law is less stringent, then HIPAA preempts the state law

For example, NYS law with respect to HIV is more stringent than HIPAA with respect to the protections it affords to patients and so NYS law prevails

# Part II
# HIPAA Privacy and Security

# Who is impacted by HIPAA?

Covered Entities (CE)

- Directly Governed by HIPAA regulations

Business Associates (BA)

- Performing work for covered entities and governed by some HIPAA regulations as a result of HITECH

Recipients of health information created, held or maintained by Covered Entities

Patients

- New "rights" under HIPAA to review information, request changes, and learn who it has been disclosed to

# What does HIPAA protect?

Health Information

- Confidentiality of Protected Health Information (Privacy/Security)
- Electronic Integrity (Security)
- Electronic Availability (Security)

Protect against "reasonably anticipated"

- Uses / disclosures of electronic information not permitted by HIPAA (Privacy/Security)
- Threats / hazards to security & integrity of electronic data (Security)

# Identifying HIPAA violations

HIPAA violations, which occur when a HIPAA requirement is violated, can be uncovered in a number of ways at either the time of their occurrence or at some later point in time. Discovery mechanisms include:

- Complaint: May be made by anyone, e.g., patient, classmate, coworker, workforce member, general public
- HHS / CMS / OCR Audits
- State Attorney General Investigations
- CE internal audit process established to comply with HIPAA Privacy/Security/Breach Reporting requirements

# Investigating HIPAA violations

- The US Office of Civil Rights (OCR) is required to investigate all HIPAA complaints it receives.
- Criminal investigations are handled by the US Department of Justice (DOJ)
- State Attorneys General may investigate complaints or conduct audits
- Covered entities are required to investigate, document and remediate any issues brought to their attention and to report breaches to HHS
- HIPAA violations may also violate State privacy laws

# Consequences of violating HIPAA

## Tiered Civil & Monetary Penalties

- Min: $100-$50,000 for each violation
- Max: not less than $50,000 for each violation
- Any violation: not more than $1,500,000 "for identical violations during a calendar year" (non-identical violations each carry a separately assessable $1.5M annual cap).

## And/or

- Knowingly misusing PHI: up to 1 year in prison
- Misuse under false pretenses: up to 5 years in prison
- Misuse with intent to sell or use for commercial gain: up to 10 years in prison

# Consequences of violating HIPAA

The Department Of Justice interprets "knowingly" for criminal liability as requiring only knowledge of the actions that constitute an offense. Specific knowledge of an action being in violation of the HIPAA statute is not required

HIPAA penalties may be applied to both the individuals responsible for the violation as well as to the covered entities or business associates in which the violation occurred

# Additional Potential Consequences

- Negative Publicity for CE and UB
- CE sanction of violator
  - The imposition of some form of sanction is required by HIPAA. These may include re-training, ejection of the individual from the CE, or the cessation of the UB program a the CE
- UB sanction of violator
  - Academic disciplinary process for students which can ultimately result in ejection from the class, program, or University

# Some key HIPAA concepts

- Covered Entity (CE)
- Business Associate (BA)
- Privacy Rule
  - Health Care
  - Health Information (HI)
  - Individually Identifiable Health Information (IHI)
  - Protected Health Information (PHI)
  - De-identified Health Information / Identifiers
  - Use / Disclosure
- Privacy Rule (cont'd)
  - Authorization
  - Accounting for Disclosures
  - Minimum Necessary
  - Treatment / Payment / Operations (TPO)
  - Notice of Privacy Practices
- Security Rule
  - Electronic Media
  - Availability / Confidentiality / Integrity
  - Administrative / Physical / Technical Safeguards

# Some key HIPAA concepts (cont'd)

- Workforce
- Workforce Training
- Workforce Sanctions
- Breach
- Breach Reporting
- Privacy & Security Officers

- Research
  - Research vs. Clinical Practice
  - Disclosure Mechanisms
    - Authorization
    - Waiver or Alteration of Authorization
    - Review Preparatory to Research
    - Research on Decedents
    - De-identified Data
    - Limited Data Set
    - Transition Provisions
  - Accounting for Disclosures
  - HIPAA + UB Policy
  - IRB role in UB HIPAA

# Covered Entity (CE) – regulated by HIPAA

a health care clearinghouse.

a health plan.

a health care provider that conducts certain transactions in electronic form.

- Currently defined in 45 CFR § 162 subparts K-S: K) Health Care Claims or Equivalent Encounter Form, L) Eligibility for a Health Plan, M) Referral Certification and Authorization, N) Health Care Claim Status, O) Enrollment and Disenrollment in a Health Plan, P) Health Care Payment and Remittance Advice, Q) Health Plan Premium Payments, R) Coordination of Benefits, S) Medicaid Pharmacy Subrogation

# Health Care Provider

Health care provider means a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

# Health Care Clearinghouse

Health care clearinghouse means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "valueadded" networks and switches, that does either of the following functions:

# Health Care Clearinghouse

(1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.

(2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

# Health Plan

Health plan means an individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg–91(a)(2)).

(The regulations go into additional detail regarding what is and is not a Health Plan which is not relevant to this presentation)

# Business Associate (BA)

A Business Associate is an entity that performs services *for* a CE involving the use or disclosure of HIPAA protected information.

HIPAA requires a Business Associate Agreement between the CE and the BA. HITECH added:

- if an entity is performing BA services for a CE, then it is a BA even if no contract is in place (e.g., as a matter of law)
- subjects BAs to HIPAA penalties if the BA does not implement elements of HIPAA applicable to a CE

# Business Associate / UB activities

Neither UB Student Training activities nor UB Research activities are Business Associate (BA) activities under HIPAA

Some covered entities incorrectly attempt to use a Business Associate Contract as a way to permit disclosure of information to UB students or researchers. Guidance on how these situations can be approached is found on the UB HIPAA web site (http://www.hpitp.buffalo.edu/hipaa/Declarations_Positions.htm). Under no circumstances should you sign a BA agreement as an individual for UB related activities

# Privacy Rule (45 CFR 164 Subpart E)

The HIPAA Privacy rule contains standards and implementation specifications designed to protect the confidentiality of patient information in any format including but not limited to electronic, paper and oral

# Privacy Rule (45 CFR 164 Subpart E)

- § 164.500 Applicability.
- § 164.501 Definitions.
- § 164.502 Uses and disclosures of protected health information: general rules.
- § 164.504 Uses and disclosures: Organizational requirements.
- § 164.506 Uses and disclosures to carry out treatment, payment, or health care operations.
- § 164.508 Uses and disclosures for which an authorization is required.
- § 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object.
- § 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.

# Privacy Rule (45 CFR 164 Subpart E)

- § 164.514 Other requirements relating to uses and disclosures of protected health information.
- § 164.520 Notice of privacy practices for protected health information.
- § 164.522 Rights to request privacy protection for protected health information.
- § 164.524 Access of individuals to protected health information.
- § 164.526 Amendment of protected health information.
- § 164.528 Accounting of disclosures of protected health information.
- § 164.530 Administrative requirements.
- § 164.532 Transition provisions.
- § 164.534 Compliance dates for initial implementation of the privacy standards.

# Health Care

Health Care means care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following:

(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and

(2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

# Health Information [HI]

Health Information means any information, whether oral or recorded in any form or medium, that: (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

# Individually Identifiable Health Information [IIHI]

Individually Identifiable Health Information is information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

# Protected Health Information [PHI]

Protected health information [PHI] means individually identifiable health information that is: (i) Transmitted by electronic media; (ii) Maintained in any medium described in the definition of electronic media; or (iii) Transmitted or maintained in any other form or medium.

Protected health information excludes individually identifiable health information in: Education records covered by the Family Educational Rights and Privacy Act (FERPA) and Employment records held by a covered entity in its role as employer.

# Protected Health Information [PHI]

It is important to understand that PHI is not just a particular kind of information. It is a particular kind of information *held by a Covered Entity.* Information classified as PHI in a CE has no particular classification outside of it and HIPAA does not regulate such information in entities which are not CEs or BAs

HIPAA only governs how PHI can be used or disclosed by the CE, including PHI in the possession of students receiving training at a CE

# De-identified Health Information

Protected Health Information that is de-identified in accordance with HIPAA requirements is no longer considered to be IIHI and so is not subject to HIPAA

# De-identified Health Information

De-identification requires either:

(1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

(i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and

(ii) Documents the methods and results of the analysis that justify such determination;

Or: removal of specific identifiers …

# De-identified Health Information

Removal of the following identifiers of the individual or of relatives, employers, or household members of the individual, from the information provided the covered entity does not have actual knowledge that the information with these identifiers removed could be used alone or in combination with other information to identify an individual who is a subject of the information:

# De-identified Health Information

The following identifiers of the individual or of relatives, employers, or household members of the individual must be removed from PHI in order to de-identify it.

(A) Names;

(B)* All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

- (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
- (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
- [Limited dataset must exclude postal address information other than town or city, state and zip code]

(C)* 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 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

(D) Telephone numbers;

(E) Fax numbers;

(F) Electronic mail addresses;

(G) Social security numbers;

(H) Medical record numbers;

(I) Health plan beneficiary numbers;

(J) Account numbers;

(K) Certificate/license numbers;

(L) Vehicle identifiers and serial numbers, including license plate numbers;

(M) Device identifiers and serial numbers;

(N) Web Universal Resource Locators (URLs);

(O) Internet Protocol (IP) address numbers;

(P) Biometric identifiers, including finger and voice prints;

(Q) Full face photographic images and any comparable images; and

(R)* Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; [creation of a unique code not disclosed to the investigator or investigator creation of such a code with a BA in place]

# De-identified information

Note identifier "R" in particular, which is a catch-all for many additional identifiers.

If a coded identifier is associated with the information it is subject to additional constraints in order for the information to be considered de-identified. The code cannot be constructed from information about the individual (including other identifiers) and if used to re-identify the individual, only the CE can have knowledge of how re-identification can be performed:

# De-identified information

(c) Implementation specifications: re-identification. A covered entity may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity, provided that:

(1) Derivation. The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and

(2) Security. The covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

# Use / Disclosure

Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information

Disclosure means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information

# HIPAA Authorization

HIPAA provides a mechanism by which a patient can authorize PHI to leave a CE, e.g., to be shared with a family member, to be used in research, etc.

The form of the authorization has many specific requirements stipulated by the HIPAA regulations. Typically the CE has an approved Authorization form. Some of the requirements include identifying who can release the information (CE), who can receive the information, and specifically what information may be released. The authorization must also note that once released, there may be no protection against subsequent re-release of the information by the recipient

# Student Disclosure of PHI

Typically, outside of Treatment/Payment/Operations, Research, or matters related to law or public health oversight, the only ways PHI may be disclosed outside of a CE are via a written authorization

For this reason students training at a CE generally may not remove PHI from the CE for any reason, including subsequent use in class

# Accounting for Disclosures

An individual (patient) has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested …

# Accounting for Disclosures

except for disclosures:

To carry out treatment, payment and health care operations

To individuals of protected health information about them

Incident to a use or disclosure otherwise permitted or required

Pursuant to an authorization

For the facility's directory or to persons involved in the individual's care or other notification purposes

# Accounting for Disclosures

except for disclosures:

For national security or intelligence purposes

To correctional institutions or law enforcement officials

As part of a limited data set; or

That occurred prior to the compliance date for the covered entity (~2003 depending on entity)

# Minimum Necessary

When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request

# Minimum Necessary (cont'd)

A covered entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when …

The information is requested by another covered entity; or

# Minimum Necessary (cont'd)

The information is requested by a professional who is a member of its workforce or is a business associate of the covered entity for the purpose of providing professional services to the covered entity, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or

Documentation or representations that comply with the applicable requirements of an IRB or Privacy Board issued waiver of authorization have been provided by a person requesting the information for research purposes

# Minimum Necessary & Students

Student training within a CE is also bound by the minimum necessary standard. Use of PHI beyond what is necessary under this requirement qualifies as a HIPAA violation

# Treatment

Treatment means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

# Payment

Payment means:

(1) The activities undertaken by:

(i) A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or

(ii) A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and

(2) The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to:

(i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

# Payment cont'd

(ii) Risk adjusting amounts due based on enrollee health status and demographic characteristics;

(iii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;

(iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

(v) Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and

# Payment cont'd

(vi) Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:

- (A) Name and address;
- (B) Date of birth;
- (C) Social security number;
- (D) Payment history;
- (E) Account number; and
- (F) Name and address of the health care provider and/or health plan.

# Operations

Health Care Operations means any of the following activities of the covered entity to the extent that the activities are related to covered functions:

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

# Operations cont'd

(2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

(3) Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable;

# Operations cont'd

(4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

(5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

(6) Business management and general administrative activities of the entity, including, but not limited to:

(i) Management activities relating to implementation of and compliance with the requirements of this subchapter;

# Operations cont'd

(ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.

(iii) Resolution of internal grievances;

(iv) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and

(v) Consistent with the applicable requirements of § 164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

# Operations cont'd

Student training while at the CE takes place a part of the CE's operations. Consequently all activity and information utilized within the CE is subject to the CE's HIPAA policies and is considered a "use".

Students may not remove ("disclose") PHI from the CE in any format including but not limited to oral, written or electronic. Bringing PHI back to UB for any purpose constitutes a non-permitted disclosure of PHI and is therefore a HIPAA violation for the CE.

# Notice of Privacy Practices [NPP]

Right to notice. An individual has a right to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information. Among other things, it must also contain new patient rights as prescribed by HIPAA

Students should familiarize themselves with the NPP of any CE the enter for training purposes. Note: HIPAA requires the NPP to be available on the CE's website if the CE has a website

# Student Use / Disclosure summary

Students may use the minimum necessary PHI as required by the educational training component of their activities only within the CE

Students may not disclose this PHI outside of the CE. Only de-identified health information may be disclosed

Permitted educational uses of PHI should be listed in the CE's NPP

# Security Rule (45 CFR 164 Subpart C)

The HIPAA Security rule contains standards and implementation specifications designed to protect the confidentiality, integrity, and availability of patient information in electronic media

# Electronic Media

Electronic media means:

(1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or

# Security Rule (45 CFR 164 Subpart C)

(2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

# Availability / Confidentiality / Integrity

Availability means the property that data or information is accessible and useable upon demand by an authorized person

Confidentiality means the property that data or information is not made available or disclosed to unauthorized persons or processes

Integrity means the property that data or information have not been altered or destroyed in an unauthorized manner

# Security Rule (45 CFR 164 Subpart C)

The Security rule standards are broken down into Administrative, Physical and Technical safeguards

*Administrative safeguards* are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.

# Security Rule (45 CFR 164 Subpart C)

*Physical safeguards* are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

*Technical safeguards* means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

# Security Rule (45 CFR 164 Subpart C)

- § 164.302 Applicability.
- § 164.304 Definitions.
- § 164.306 Security standards: General rules.
- § 164.308 Administrative safeguards.
- § 164.310 Physical safeguards.
- § 164.312 Technical safeguards.
- § 164.314 Organizational requirements.
- § 164.316 Policies and procedures and documentation requirements.
- § 164.318 Compliance dates for the initial implementation of the security standards.

Appendix A to Subpart C of Part 164—Security Standards: Matrix

# Security Rule

Security Rule Implementation Specifications within HIPAA are either (R)=Required, or (A)=Addressable

Addressable means the covered entity can assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity's electronic protected health information; and

# Security Rule cont'd

(ii) As applicable to the entity—

(A) Implement the implementation specification if reasonable and appropriate; or

(B) If implementing the implementation specification is not reasonable and appropriate—

(1) Document why it would not be reasonable and appropriate to implement the implementation specification; and

(2) Implement an equivalent alternative measure if reasonable and appropriate.

# Security Rule – more detail

- § 164.308 Administrative safeguards.
- § 164.310 Physical safeguards.
- § 164.312 Technical safeguards.

# Administrative safeguards 45 CFR 164.308

Security Management Process 164.308(a)(1)

- Risk Analysis (R), Risk Management (R), Sanction Policy (R), Information System Activity Review (R)

Assigned Security Responsibility 164.308(a)(2) (R)

Workforce Security 164.308(a)(3)

- Authorization and/or Supervision (A), Workforce Clearance Procedure (A), Termination Procedures (A)

Information Access Management 164.308(a)(4)

- Isolating Health care Clearinghouse Function (R), Access Authorization (A), Access Establishment and Modification (A)

# Administrative safeguards 45 CFR 164.308

Security Awareness and Training 164.308(a)(5)

- Security Reminders (A), Protection from Malicious Software (A), Log-in Monitoring (A), Password Management (A)

Security Incident Procedures 164.308(a)(6)

- Response and Reporting (R)

Contingency Plan 164.308(a)(7)

- Data Backup Plan (R), Disaster Recovery Plan (R), Emergency Mode Operation Plan (R), Testing and Revision Procedure (A), Applications and Data Criticality Analysis (A)

# Administrative safeguards 45 CFR 164.308

Evaluation 164.308(a)(8) (R)

Business Associate Contracts and Other Arrangement 164.308(b)(1)

- Written Contract or Other Arrangement (R)

# Physical safeguards 45 CFR 164.310

Facility Access Controls 164.310(a)(1)

- Contingency Operations (A), Facility Security Plan (A), Access Control and Validation Procedures (A), Maintenance Records (A)

Workstation Use 164.310(b) (R)

Workstation Security 164.310(c) (R)

Device and Media Controls 164.310(d)(1)

- Disposal (R), Media Re-use (R), Accountability (A), Data Backup and Storage (A)

# Technical safeguards 45 CFR 164.312

Access Control 164.312(a)(1)

- Unique User Identification (R), Emergency Access Procedure (R), Automatic Logoff (A), Encryption and Decryption (A)

Audit Controls 164.312(b) (R)

Integrity 164.312(c)(1)

- Mechanism to Authenticate Electronic Protected Health Information (A)

Person or Entity Authentication 164.312(d) (R)

Transmission Security 164.312(e)(1)

- Integrity Controls (A), Encryption (A)

# Workforce

Workforce means Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a CE, is under the direct control of such entity, whether or not they are paid by the CE

Students training is a Healthcare Operations activity of the CE under HIPAA and students are considered part of the CE workforce per separate Student Clinical Affiliation Agreements between the CE and UB for formal UB educational programs

# Workforce Training required

- 164.308(a)(5)(i) Standard: Security awareness and training. Implement a security awareness and training program for all members of its workforce (including management).
- 164.530(b)(1) Standard: Training. A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart [Privacy] and subpart D [Breach Notification] of this part, as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity.

# Workforce Training required

§ 164.530(b)(2) *Implementation specifications: Training.*

(i) A covered entity must provide training that meets the requirements of paragraph (b)(1) of this section, as follows:

- (A) To each member of the covered entity's workforce by no later than the compliance date for the covered entity;
- (B) Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and
- (C) To each member of the covered entity's workforce whose functions are affected by a material change in the policies or procedures required by this subpart or subpart D of this part, within a reasonable period of time after the material change becomes effective in accordance with paragraph (i) of this section.

# Workforce Training required

(ii) A covered entity must document that the training as described in paragraph (b)(2)(i) of this section has been provided, as required by paragraph (j) of this section.

# CE HIPAA Training

If you have questions about HIPAA training, policies or procedures specific to the institution where you are studying or working you can (and should) contact the institution's HIPAA Privacy or Security officers for additional guidance

UB does not want its faculty and students inadvertently causing HIPAA violations for institutions they are working with. As there are over 3,000 such intuitions, each revising its own HIPAA policies as it sees fit, only the institutions can provide this training

# Workforce Sanctions required

- § 164.308(a)(1)(ii)(C) Sanction policy (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.

- § 164.530(e)(1) Standard: Sanctions. A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart or subpart D of this part. This standard does not apply to a member of the covered entity's workforce with respect to actions that are covered by and that meet the conditions of § 164.502(j) or paragraph (g)(2) of this section. (2) Implementation specification: Documentation. As required by paragraph (j) of this section, a covered entity must document the sanctions that are applied, if any.

# Breach § 164.400

Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E (Privacy Rule) of this part which compromises the security or privacy of the protected health information.

# Breach - Definition

(1)(i) For purposes of this definition, compromises the security or privacy of the protected health information means poses a significant risk of financial, reputational, or other harm to the individual.

(ii) A use or disclosure of protected health information that does not include the identifiers listed at § 164.514(e)(2) [Limited data set], date of birth, and zip code does not compromise the security or privacy of the protected health information.

# Breach - Exclusion

(2) Breach excludes:

(i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.

# Breach - Exclusion

(ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.

# Breach - Exclusion

(iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

# Breach – encryption "safe harbor"

A Breach has not occurred if the information involved was rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) [HITECH] of Public Law 111–5 on the HHS Web site.

For example, loss of a laptop containing PHI is not a breach if the laptop was encrypted in compliance with the above standards and only the CE possess the decryption keys

# Breach Notification

A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.

# Breach Discovered

A breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency). With limited exception a covered entity shall provide the notification without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

# Breach – HHS reporting ≥ 500

For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach, notify prominent media outlets serving the State or jurisdiction. For purposes of this section, State includes American Samoa and the Northern Mariana Islands.

Breaches must also, at the same time, be reported to HHS and will appear on a web site: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html

# Breach – HHS reporting < 500

For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide this documentation to HHS.

# Breach – Your Obligations

If you are aware of a suspected Breach, caused either by yourself or someone else, report it immediately to the CE's HIPAA officials

# Security & Privacy Officers

**(Security Officer) § 164.308(a)(2)** *Standard: Assigned security responsibility.* Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.

**(Privacy Officer) § 164.530** (a)(1) *Standard: Personnel designations.* (i) A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity. (ii) A covered entity must designate a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the notice required by § 164.520.

# Key Points for Students

- HIPAA *never* prevents sharing of PHI for treatment purposes
- Know what Protected Health Information is and how it may be de-identified
- Restrict your use of PHI to the minimum necessary to accomplish a specific task
- PHI should not be removed from the CE. If PHI is removed in a way not permitted by HIPAA both the student and CE are potentially exposed to significant penalties at the Federal, State and local (CE, UB) levels.

# Key Points for Students

- Students training at a CE are part of the CE workforce while at the CE and are governed by CE HIPAA policies/procedures
- Students must receive a general orientation to HIPAA from UB and must *also* receive training specific to their activities at the CE from the CE
- If you have questions about what is permissible at a CE or become aware of a possible HIPAA violation, notify your instructor as well as the CE's HIPAA Privacy or Security officers

# Part III
# HIPAA and Research

This section deals with the impact of HIPAA on research conducted within Covered Entities in the context of UB's research function which is *not* regulated by HIPAA

# HIPAA defines Research

*Research* means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge

# Does HIPAA apply to Research?

"The Privacy Rule does not apply to research; it applies to covered entities, which researchers may or may not be. The rule may affect researchers because it may affect their access to information, but it does not regulate them or research, per se."

"Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule"; Department of Health and Human Services; pg 5 (no document date; distributed at AHEC conference Fall, 2005)

# Research vs. Clinical Practice

"*Part A: Boundaries Between Practice & Research*" of the April 18, 1979 Bellmont report

"It is important to distinguish between biomedical and behavioral research, on the one hand, and the practice of accepted therapy on the other …" "The distinction between research and practice is blurred partly because both often occur together (as in research designed to evaluate a therapy) and partly because notable departures from standard practice are often called "experimental" when the terms "experimental" and "research" are not carefully defined."

# Research vs. Clinical Practice

"For the most part, the term "practice" refers to interventions that are designed solely to enhance the well-being of an individual patient or client and that have a reasonable expectation of success. The purpose of medical or behavioral practice is to provide diagnosis, preventive treatment or therapy to particular individuals."

# Research vs. Clinical Practice

"By contrast, the term 'research' designates an activity designed to test an hypothesis, permit conclusions to be drawn, and thereby to develop or contribute to generalizable knowledge (expressed, for example, in theories, principles, and statements of relationships). Research is usually described in a formal protocol that sets forth an objective and a set of procedures designed to reach that objective."

# Research vs. Clinical Practice

Under HIPAA Clinical Practice (treatment) and Research are two separate activities that may occur simultaneously. HIPAA explicitly places Research outside the protected CE boundaries of Treatment, Payment and Operations.

This means that a Research activity within a CE cannot use CE PHI unless the PHI is obtained via one of seven PHI access mechanisms defined by HIPAA. *This requirement holds even for a physician wishing to use her own patient's PHI for research*

# HIPAA PHI and Research

HIPAA provides 7 "keys" to accessing PHI held by a CE for research use

These Keys permit PHI to move from covered entity treatment side to a research activity (inside or outside of a CE).

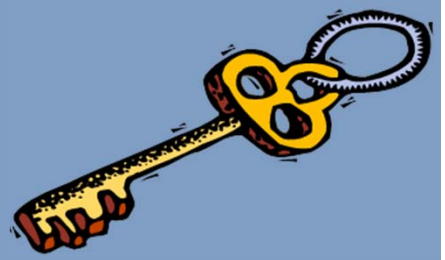
Implementation of some keys and activities related to them is dependent on whether researcher is within the covered entity holding the PHI.

# Ability to access PHI ≠ HIPAA Approved

The mere ability to access CE PHI, either as a consequence of having a direct treatment relationship with the subject of the PHI, or related legitimate TPO access to medical records, is *not* a HIPAA approved mechanism for acquiring PHI for use in research.

Using PHI for research outside of one of the legitimate HIPAA research PHI transfer mechanisms creates liability for CEs holding the PHI *and* the researcher under HIPAA's penalty structure.

# Research Access to PHI



**Authorization**

45 CFR § 164.508

Waiver or Alteration of Authorization

Review Preparatory to Research

Research on Decedents

De-identified Data

Limited Data Set

Transition Provisions

# Authorization

HIPAA allows the subject of PHI to sign an authorization allowing disclosure of their PHI to a researcher. This authorization may be stand-alone or embedded in the informed consent†. HIPAA has many requirements that the written authorization must meet. These can be reviewed here:

http://www.hpitp.buffalo.edu/hipaa/Research/authorizations.htm

†Authorizations for release of psychotherapy notes must be stand-alone and cannot be embedded in the informed consent. New York state sets additional requirements for certain types of health information

# Research Access to PHI

Authorization

**Waiver or Alteration of Authorization**

45 CFR § 164.512(i)(1)(i)

Review Preparatory to Research

Research on Decedents

De-identified Data

Limited Data Set

Transition Provisions

# Waiver or Alteration of Authorization

- HIPAA permits an IRB to alter or waive individual requirements for the HIPAA authorization under certain circumstances when obtaining written authorization is not practicable. A documented IRB action of this nature may be relied upon by a CE to release PHI in a HIPAA compliant fashion.
- A copy of the IRB alteration or waiver should be provided to the CE as they must be able to document this in the event of an OCR audit or investigation

# Waiver or Alteration of Authorization

Circumstances requiring a waiver can include:

- Retrospective medical records research
- Screening medical records to identify potential study candidates
- Recruiting subjects to a protocol based on PHI from a covered entity

The application to be submitted to the IRB requesting an alteration or waiver can be found here:

www.hpitp.buffalo.edu/hipaa/Research/waiver_of_authorization.htm

# CE Policies on Subject Recruitment

Local hospitals affiliated with UB additionally require that the initial approach to subjects for recruitment, based on PHI obtained from the hospitals via a waiver, occur through a member of the patient's immediate treatment team.

Although this is not required by HIPAA, hospitals implement this policy in order to avoid potentially upsetting patients when an unknown individual (researcher) approaches them with knowledge of their individual health information

# Research Access to PHI

Authorization

Waiver or Alteration of Authorization

**Review Preparatory to Research**

45 CFR § 164.512(i)(1)(ii)

Research on Decedents

De-identified Data

Limited Data Set

Transition Provisions

# Review Preparatory to Research

Investigators who are also members of a Covered Entity Workforce may use this mechanism as long as:

- Use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research;
- No protected health information is to be removed from the covered entity by the researcher in the course of the review; and
- The protected health information for which use or access is sought is necessary for the research purposes.

# Review Preparatory to Research

UB has a form that investigators can use to document this mechanism for a CE. It is available here:

www.hpitp.buffalo.edu/hipaa/Research/reviews_preparatory_to_research.htm

# Research Access to PHI

Authorization

Waiver or Alteration of Authorization

Review Preparatory to Research

**Research on Decedents**

45 CFR § 164.512(i)(1)(iii)

De-identified Data

Limited Data Set

Transition Provisions

# Research on Decedents

Investigators may obtain decedent PHI with this mechanism as long as they provide a CE with:

- (A) Representation that the use or disclosure sought is solely for research on the protected health information of decedents;
- (B) Documentation, at the request of the covered entity, of the death of such individuals; and
- (C) Representation that the protected health information for which use or disclosure is sought is necessary for the research purposes.

# Research on Decedents

UB has a form that investigators can use to document this mechanism for a CE. It is available here:

www.hpitp.buffalo.edu/hipaa/Research/research_on_decedents.htm

# Research Access to PHI

Authorization

Waiver or Alteration of Authorization

Review Preparatory to Research

Research on Decedents

**De-identified Data**

45 CFR § 164.514(a-c)

Limited Data Set

Transition Provisions

# IRB Anonymous ≠ HIPAA de-identified

Be aware that some forms of health information which qualify as PHI may also qualify as "anonymous" by IRB standards. For this reason it is possible that a protocol determined to be anonymous by the IRB will still require the investigator to identify a HIPAA transfer mechanism for acquiring PHI. PHI is not de-identified unless it complies with the prescribed HIPAA de-identification requirements

# De-identified Data

Data that meets the HIPAA standard for being de-identified is not protected by HIPAA.

De-identification requires:

- the removal (currently) of 18 identifiers of the individual or of relatives, employers, or household members of the individual. And the 18th identifier ("R") is a catch-all for many additional identifiers
- The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

# De-identified Health Information

The following identifiers of the individual or of relatives, employers, or household members of the individual must be removed from PHI in order to de-identify it.

(A) Names;

(B)* All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

- (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
- (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
- [Limited dataset must exclude postal address information other than town or city, state and zip code]

(C)* 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 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

(D) Telephone numbers;

(E) Fax numbers;

(F) Electronic mail addresses;

(G) Social security numbers;

(H) Medical record numbers;

(I) Health plan beneficiary numbers;

(J) Account numbers;

(K) Certificate/license numbers;

(L) Vehicle identifiers and serial numbers, including license plate numbers;

(M) Device identifiers and serial numbers;

(N) Web Universal Resource Locators (URLs);

(O) Internet Protocol (IP) address numbers;

(P) Biometric identifiers, including finger and voice prints;

(Q) Full face photographic images and any comparable images; and

(R)* Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; [creation of a unique code not disclosed to the investigator or investigator creation of such a code with a BA in place]

# De-identified Data

A covered entity may assign a code or other means of record identification to allow de-identified data to be re-identified by the covered entity, provided that:

(1) Derivation. The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and

(2) Security. The covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

# Data De-identification

An investigator who is a member of the workforce of the CE holding the PHI may perform the de-identification and then use the de-identified data for research purposes

An investigator who is not part of the CE will need the CE to perform the de-identification. If the CE cannot do this, the investigator will need UB to execute a Business Associate Agreement with the CE allowing the investigator to perform the de-identification. More information is available here: www.hpitp.buffalo.edu/hipaa/Research/DataExtraction.htm

# Research Access to PHI

Authorization

Waiver or Alteration of Authorization

Review Preparatory to Research

Research on Decedents

De-identified Data

Limited Data Set

45 CFR § 164.514(e)

Transition Provisions

# Limited Dataset

A limited data set is PHI that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

(i) Names; (ii) Postal address information, other than town or city, State, and zip code; (iii) Telephone numbers; (iv) Fax numbers; (v) Electronic mail addresses; (vi) Social security numbers; (vii) Medical record numbers; (viii) Health plan beneficiary numbers; (ix) Account numbers; (x) Certificate/license numbers; (xi) Vehicle identifiers and serial numbers, including license plate numbers; (xii) Device identifiers and serial numbers; (xiii) Web Universal Resource Locators (URLs); (xiv) Internet Protocol (IP) address numbers; (xv) Biometric identifiers, including finger and voice prints; and (xvi) Full face photographic images and any comparable images.

# Data Use Agreement

A Limited Data Set may only be used for the purposes of research, public health, or health care operations, and must be accompanied by a Data Use Agreement

The Data Use Agreement requires institutional review and signature. UB has not delegated signature authority for the Data Use Agreement to individual investigators

# Research Access to PHI

Authorization

Waiver or Alteration of Authorization

Review Preparatory to Research

Research on Decedents

De-identified Data

Limited Data Set

Transition Provisions

45 CFR § 164.532

# Transition Provisions ("Grandfathering")

Permits the use and disclosure of PHI created or received before or after April 14, 2003 if one of the following was obtained prior to that date:

- An authorization or other express legal permission from an individual to use or disclose protected health information for the research;
- The informed consent of the individual to participate in the research; or
- A waiver, by an IRB, of informed consent.

If subjects must be re-consented these provisions turn off and there must be an valid HIPAA transfer mechanism put in place at that time

# Research impacts on CE

Beyond ensuring that PHI from a CE has an appropriate transfer mechanism in place in order to use it for research purposes, HIPAA places some additional burdens on the CE that vary by mechanism

The investigator should ensure that these requirements will be satisfied before using PHI

- Minimum Necessary
- Accounting for Disclosures

# PRIVACY RULE CE REQUIREMENTS

| | MINIMUM NECESSARY | ACCOUNTING |
|---|---|---|
| Authorization | No | No |
| Waiver of Authorization | Yes | Yes * |
| Preparatory Reviews | Yes | Yes |
| Decedent PHI | Yes | Yes |
| Limited Data Set | Yes | No |
| De-identification | No | No |
| Transition Provisions | Yes | Yes |

*Modified Accounting for Research Disclosures may be used for studies involving disclosures of 50 or more individuals

# UB Research Function & HIPAA

The UB research function, and the data it holds, is not regulated by HIPAA

- UB is part of the SUNY Hybrid HIPAA Covered Entity
- UB determines, guided by the regulations, which functions are covered by HIPAA and which are not
- Faculty engage in research as a UB activity, not as a practice plan, hospital, or other CE activity
- UB has defined its research activity as not being part of any UB/SUNY covered function
- As a consequence of this designation, HIPAA only impacts UB research when PHI is transferred from a CE or "provision of healthcare" setting to the UB researcher

# HIPAA + local (UB) Policy

HIPAA requires a release mechanism be in place when PHI is Used or Disclosed by a covered entity for research purposes

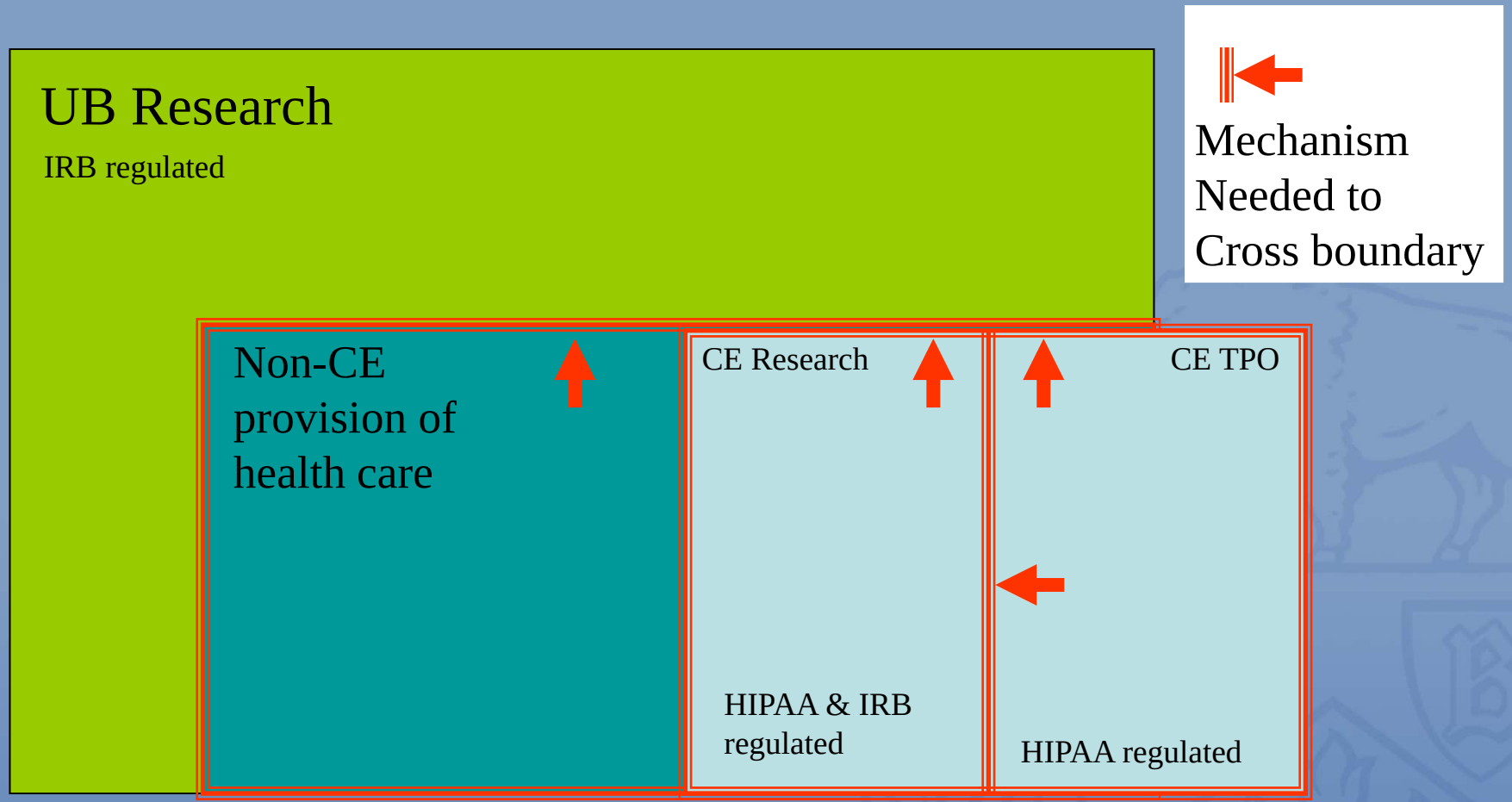
UB extends this requirement to cover all research approved by the UB IRBs, or performed by a UB researcher, involving the provision of Health Care and Individually Identifiable Health Information so that the same kind of information does not receive different protections based solely on the source of the information

# HIPAA / IRB / UB

The HIPAA regulations prescribe only one duty to the IRB, and that is to issue a Waiver or Alteration of the Authorization requirement when appropriate

UB policy has expanded the role of the IRB to review protocols and ensure that a HIPAA transfer mechanism is in place when needed. In addition to providing uniform protection for similar types of data, this policy also eliminates the need for the researcher or the IRB to engage in the 'is there a CE?' analysis for each protocol. If the protocol is IRB approved, the mechanisms required of a CE will automatically be in place

# UB IRB Boundaries requiring PHI release mechanisms for research use

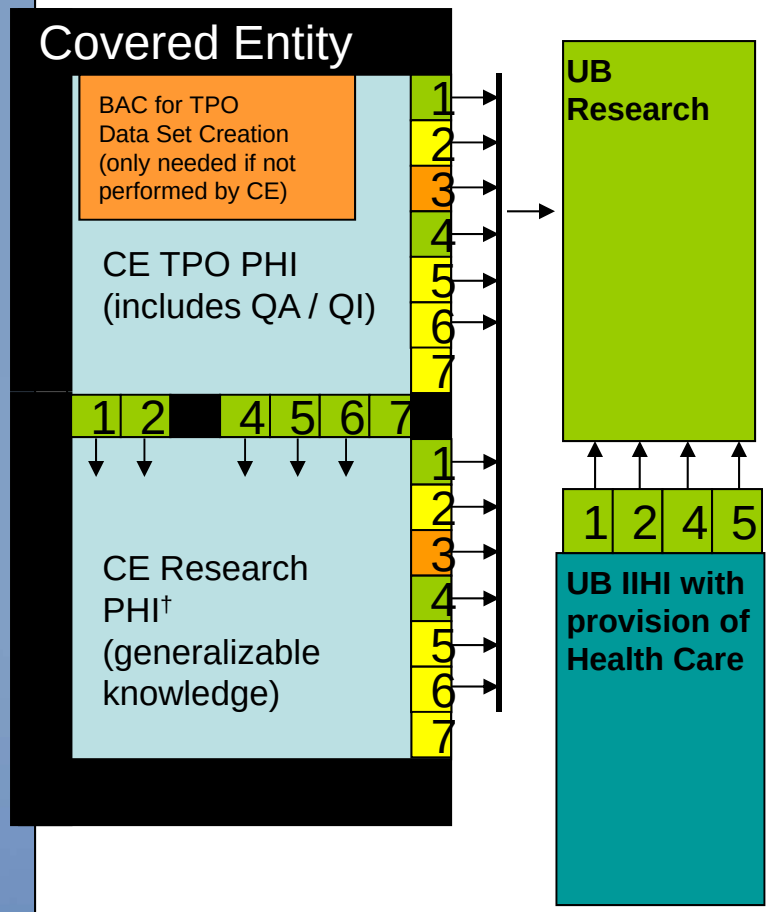


# Transfer mechanism summary

The following slide schematically illustrates the various transfer mechanisms and how they can be used within or outside of a HIPAA covered entity

- The black box on the left represents a covered entity and is partitioned into two areas. On the top is where PHI from Treatment/Payment/Operations resides. On the bottom is where PHI in research activities conducted by the CE (not UB or a UB researcher) resides
- All research conduced by UB researchers resides in the green box on the right

# UB+HIPAA Research PHI "Release"




† Does not occur within UB CE

## Research specific release mechanisms:

Every single piece of research PHI from a CE for use within the CE (by the CE), or outside of the CE (by a UB researcher), must be obtained through one of these mechanisms

- "Inside" CE; full HIPAA protections
- No additional HIPAA requirements*
- Disclosure accounting
- Contractual requirements (entity to entity)

1 - Authorization
2 - Waiver or Alteration of Authorization
3 - Limited Data Set + Data Use Agreement (contract)
4 - De-Identified Data
5 - Research on Decedents
6 - Transition Provisions
7 - Reviews Preparatory to Research
(no PHI removed from CE or used in research itself)
(only CE workforce can use for subject recruitment)

* Requirements associated with release mechanism (if any) remain in force

# Which transfer mechanism to use?

HIPAA does not prescribe which transfer mechanism should be utilized when more than one mechanism can be used

To simplify things for the investigator and minimize the need for legal counsel review of documents (by the CE and UB), UB has placed an emphasis on using De-identification, Authorization, or IRB Waiver/Alteration of Authorization as these mechanisms cover most protocols. A worksheet is available for investigator use to determine the most appropriate mechanism for their protocol:

www.hpitp.buffalo.edu/hipaa/Research/HIPAA_InvestigatorDataAccessWorksheet.htm

# Covered Entity Considerations

Creation of Research Record Set

- Who can do this?
- Minimum necessary

Releasing Research Record Set to researcher

- Validation & documentation of release mechanism, adherence to minimum necessary and accounting for disclosure requirements

# Research Record Set Creation

By covered entity workforce (with approved release mechanism ready to exercise)

- Staff physician
- Workforce member

By Business Associate for non-workforce member

- External PI
- Research team member
  - UBF, RF, SUNY, Clinical Practice Plan

# Research Record Set Release

By covered entity workforce (with approved release mechanism ready to exercise and CE retaining documentation of the mechanism)

By Business Associate for non-workforce member if permitted, *and then only according to specifications of the Business Associate Agreement*

# HIPAA Path for Investigators

Use UB's *HIPAA Worksheet* to determine if a HIPAA transfer mechanism is required for the protocol (http://www.hpitp.buffalo.edu/hipaa/Research/HIPAA_InvestigatorDataAccessWorksheet.htm)

If health care and identifiable health information are involved, IRB ensures that investigator has identified one of the HIPAA transfer mechanisms before approving protocol

- Covered Entities are independently responsible for ensuring these mechanisms are in place before permitting the release of PHI to a UB researcher

# HIPAA Path for Investigators

If a researcher will be performing the data extraction from a CE and is not a member of the CE workforce, they perform this activity as a Business Associate

A Business Associate Agreement must be executed between the CE and UB at an institutional level (SUNY / UBFA / RF). Investigators may not execute these agreements on their own

Business Associates are subject to HIPAA and its associated penalties *by law, even if a HIPAA Business Associate Agreement is not in place*

# Signature Authority

It is important to note that signature authority for HIPAA contractual documents requiring signature, i.e., the Data Use Agreement and the Business Associate Agreement, has not been delegated to individual investigators. Documents of this nature require an institutional signature

Contact UB's Office of HIPAA Compliance if you are presented with such documents and asked to execute them (hipaa-compliance@buffalo.edu)

# More information

* IRB

* Online (from base url www.hpitp.buffalo.edu/hipaa)

- /UB_HIPAA_ResearchHomePage.htm
- /Research/HIPAA_InvestigatorDataAccessWorksheet.htm
- /Declarations_Positions.htm

UB office of HIPAA compliance

- hipaa-compliance@buffalo.edu

Centers for Medicare and Medicaid Services

- www.cms.hhs.gov/HIPAAGenInfo/