HIPAA at UB
Clinical, Educational and Research Implications

Brian Murphy
UB Director of HIPAA Compliance
bwmurphy@buffalo.edu

Who is Impacted by HIPAA

- Covered Entities
  - Governed by regulations
- Recipients of information from Covered Entities
  - Covered entity constrained in terms of what PHI it can release, and under what conditions.
- Patients
  - New “rights” under HIPAA

What does HIPAA protect?

- 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)

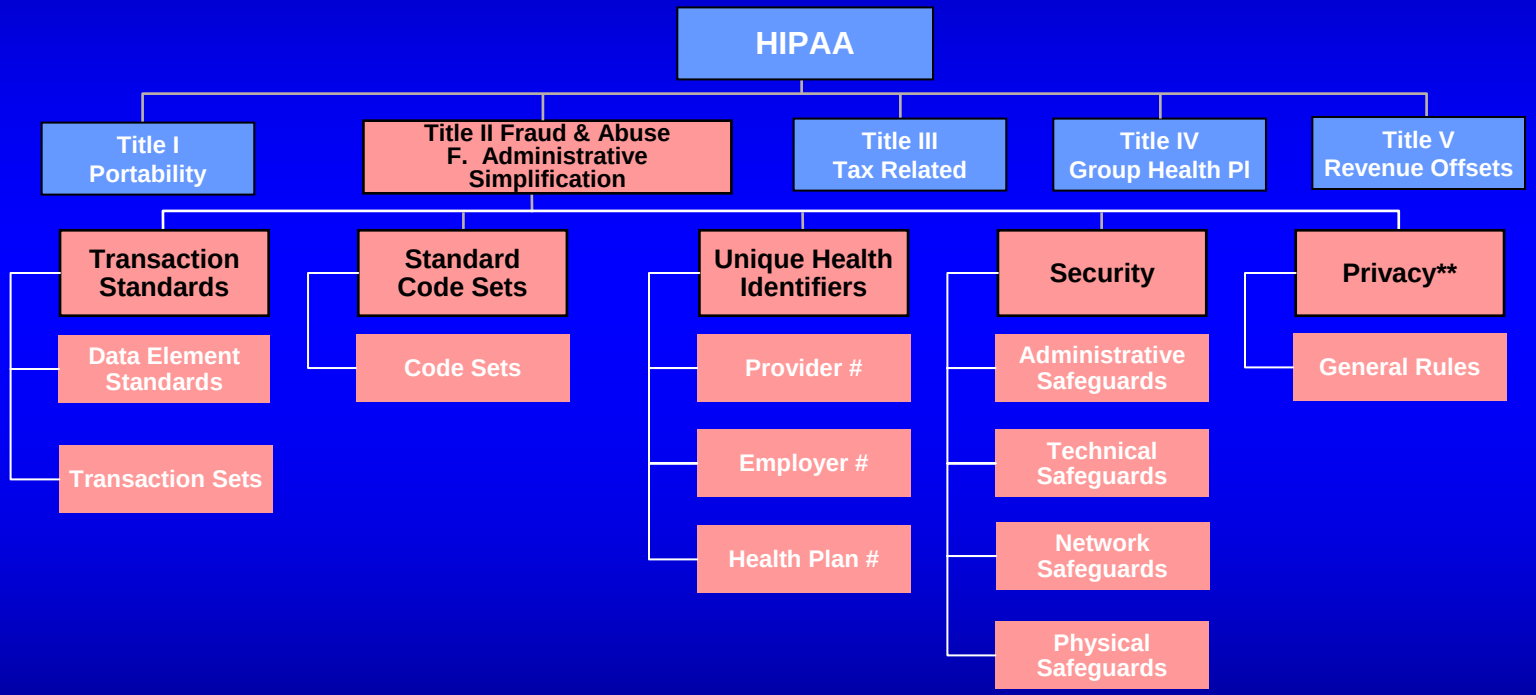
Consequences of violating HIPAA

- Complaint Driven
- Civil & Monetary Penalties
  - $100/"person"/specific violation
    - Max $25,000 per specific violation/year
  - Knowingly misusing PHI: up to $50,000 and/or 1 year in prison
  - Misuse under false pretenses: up to $100,000 and/or 5 years in prison
  - Misuse with intent to sell or use for commercial gain: up to $250,000 and/or up to 10 years in prison
- Negative Publicity
- Employer sanctions (some form of sanction required by HIPAA)
- Enforcement: OCR; CMS; DOJ

Implementing HIPAA

- CE Responsibility
  - UB provides general orientation to students placed in CE settings
- GAP Analysis
- Risk Assessment
- Policies / Procedures / Practices
- Training, Training, Training
- Documentation, Documentation, Documentation

Background: HIPAA has many parts



HIPAA Administrative Simplification

- **Transactions & Code Sets 10/16/2002 (10/16/2003 with extension)**
  - Standardizing electronic transactions to save costs, minimize complexity, and simplify identification of misconduct
  - Electronic Signature (proposed rule)
- **Privacy (4/14/2003)**
  - Ensure that patient information (elements that belong in the medical record, stored or transmitted in any form) is not released beyond the realm of treatment/payment/operations without explicit patient permission or an accounting mechanism enabling the patient to identify releases.
- **Security (4/20/2005)**
  - Ensure that electronically maintained patient information is protected against unintended access/loss/modification and is available even under 'emergency conditions'.
- **Identifiers**
  - Employer: (7/30/2004) employer's tax ID number or Employer Identification Number (EIN)
  - Provider: (5/23/2007) National Provider Identifier (NPI)
  - Health Plans: (proposed)
  - Individual Identifiers (dropped; may be revived)

Some key HIPAA Privacy concepts

- **Covered Entity**
- Notice of Privacy Practices
- Workforce
- Treatment / Payment / Operations
- Health Information
- Individually Identifiable Health Information
- Protected Health Information
- Use vs. Disclosure
- Accounting for Disclosures
- Minimum Necessary

Covered Entity

- 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-R: 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

UB Covered Entity

- Hybrid Entity (UB/SUNY)
- UB CE: School of Dental Medicine clinic operations
- UB Non-CE: Everything Else
  - Student Health Clinic
  - Sub-Board I Pharmacy
  - Medical School Faculty
  - Any UB Research Activity
  - Speech-Language and Hearing Clinic
- Multiple roles: some may be part of CE, others not

Some key HIPAA Privacy concepts

- Covered Entity
- **Notice of Privacy Practices**
- Workforce
- Treatment / Payment / Operations
- Health Information
- Individually Identifiable Health Information
- Protected Health Information
- Use vs. Disclosure
- Accounting for Disclosures
- Minimum Necessary

Notice of Privacy Practices

- *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:
  - (A) The right to request restrictions on certain uses and disclosures of protected health information;
  - (B) The right to receive confidential communications of protected health information;
  - (C) The right to inspect and copy protected health information;
  - (D) The right to amend protected health information;
  - (E) The right to receive an accounting of disclosures of protected health information;
  - (F) The right to receive a written copy of the Notice of Privacy Practices

Some key HIPAA Privacy concepts

- Covered Entity
- Notice of Privacy Practices
- **Workforce**
- Treatment / Payment / Operations
- Health Information
- Individually Identifiable Health Information
- Protected Health Information
- Use vs. Disclosure
- Accounting for Disclosures
- Minimum Necessary

Workforce

- *Workforce* means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.
  - Students visiting a CE under a clinical affiliation agreement are members of that CE's workforce while at that CE and must follow the CE's prescribed HIPAA policies/procedures.

Some key HIPAA Privacy concepts

- Covered Entity
- Notice of Privacy Practices
- Workforce
- **Treatment / Payment / Operations**
- Health Information
- Individually Identifiable Health Information
- Protected Health Information
- Use vs. Disclosure
- Accounting for Disclosures
- Minimum Necessary

Treatment / Payment / Operations

- *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

- (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

Payment

- (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;
  - (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
  - (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;
- (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;
- (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; (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 deidentified health information or a limited data set, and fundraising for the benefit of the covered entity.

Some key HIPAA Privacy concepts

- Covered Entity
- Notice of Privacy Practices
- Workforce
- Treatment / Payment / Operations
- **Health Information**
- **Individually Identifiable Health Information**
- **Protected Health Information**
- Use vs. Disclosure
- Accounting for Disclosures
- Minimum Necessary

HI

Privacy: § 160.103 Health Information

- 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.

HI→IIHI

Privacy: § 160.103 Individually Identifiable Health Information

- Individually identifiable health information [IIHI] 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.

HI → IIHI → PHI

Privacy: § 160.103 Protected Health Information

- Protected health information [PHI] means individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: (i) Transmitted by electronic media; (ii) Maintained in any medium described in the definition of electronic media at § 162.103 of this subchapter; or (iii) ***Transmitted or maintained in any other form or medium***. (2) Protected health information ***excludes*** individually identifiable health information in: (i) Education ***records covered by the Family Educational Rights and Privacy Act***, as amended, 20 U.S.C. 1232g; (ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and (iii) ***Employment records held by a covered entity in its role as employer***.

Protected Health Information

[Privacy: §164.514(b)(2)(i)] De-identification criteria

The following identifiers of the individual or of relatives, employers, or household members of the individual:
(* Indicates permitted in a limited dataset §164.514(e)(2))

(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]

Some key HIPAA Privacy concepts

- Covered Entity
- Notice of Privacy Practices
- Workforce
- Treatment / Payment / Operations
- Health Information
- Individually Identifiable Health Information
- Protected Health Information
- **Use vs. Disclosure**
- Accounting for Disclosures
- Minimum Necessary

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.

Some key HIPAA Privacy concepts

- Covered Entity
- Notice of Privacy Practices
- Workforce
- Treatment / Payment / Operations
- Health Information
- Individually Identifiable Health Information
- Protected Health Information
- Use vs. Disclosure
- **Accounting for Disclosures**
- Minimum Necessary

Accounting for Disclosures

(a) Standard: right to an accounting of disclosures of protected health information.

(1) An individual 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, except for disclosures:

(i) To carry out treatment, payment and health care operations

(ii) To individuals of protected health information about them

(iii) Incident to a use or disclosure otherwise permitted or required

(iv) Pursuant to an authorization

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

(vi) For national security or intelligence purposes

(vii) To correctional institutions or law enforcement officials

(viii) As part of a limited data set; or

(ix) That occurred prior to the compliance date for the covered entity.

Some key HIPAA Privacy concepts

- Covered Entity
- Notice of Privacy Practices
- Workforce
- Treatment / Payment / Operations
- Health Information
- Individually Identifiable Health Information
- Protected Health Information
- Use vs. Disclosure
- Accounting for Disclosures
- **Minimum Necessary**

Minimum Necessary

(1) *Minimum necessary applies.* 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

- 45 CFR §164.514(d)(3)(iii)(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 …

Minimum Necessary

- (B) The information is requested by another covered entity;
- (C) 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
- (D) Documentation or representations that comply with the applicable requirements of § 164.512(i) [waiver of authorization] have been provided by a person requesting the information for research purposes.

Notes:

- Understanding some key concepts and what they encompass is important
- HIPAA lets PHI flow freely when it is for the purposes of TPO (HIPAA *never* prevents sharing of PHI for treatment purposes)
- HIPAA does not let PHI flow beyond TPO except in well defined ways that you should be able to identify before using them.

HIPAA and Research

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."

"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

"Research and practice may be carried on together when research is designed to evaluate the safety and efficacy of a therapy."

NB: Clinical Practice (treatment) and Research are two separate activities that often occur simultaneously. HIPAA *explicitly* places Clinical Practice within TPO while placing Research outside of TPO. Human Subject Research always requires IRB review.

HIPAA PHI and Research

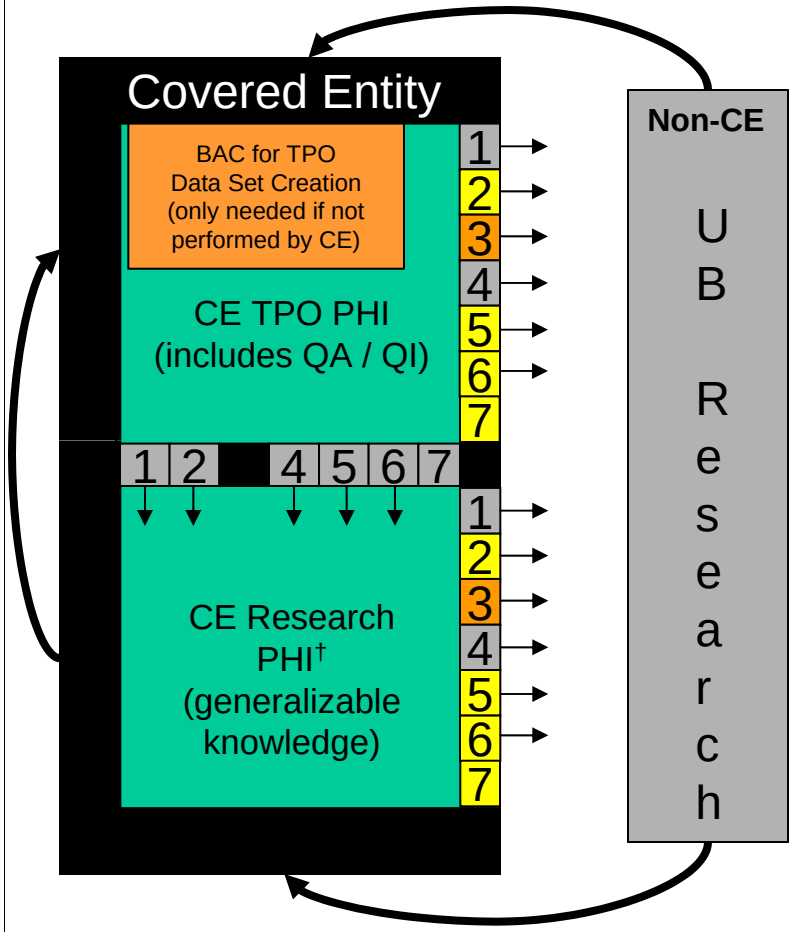
- HIPAA provides 7 “keys” to accessing PHI.
- Keys permit PHI to move from covered entity treatment side to researchers (in or out of CE).
- Implementation of some keys and activities related to them is dependent on whether researcher is within the covered entity holding the PHI.

WHAT DOES THE PRIVACY RULE REQUIRE?

	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 Tracking* may be used for studies involving disclosures of 50 or more individuals

HIPAA Covered Entity Research PHI "Release" mechanisms & requirements



† 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 can use for subject recruitment)

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

HIPAA + local (UB) Policy

- HIPAA requires a release mechanism be in place when information is used/disclosed by a covered entity for research purposes.
- UB extends this requirement to cover all research (performed by UB researchers) so that the same kind of information does not receive different protections based solely on where it came from. This also eliminates the need to engage in ‘is there a CE?’ analysis.

The “simple” slide

- HIPAA & Research at UB
  - Research involving provision of health care or individually identifiable health information will require a “release” mechanism to possess/use that information for research purposes.
  - The IRB can tell you which mechanism you will need, or you can determine this for yourself on-line: http://www.hpitp.buffalo.edu/hipaa/HIPAA_InvestigatorDataAccessWorksheet.htm

Most confusing aspect – multiple roles

- Clinicians perform Treatment/Payment/Operations as part of their professional obligation to some covered entity (hospital, practice plan, dental clinic)
- Researchers perform research activities as part of professional obligation to UB
- Clinicians, Researchers and Students are often the same people
  - Don’t confuse roles (TPO access to PHI as clinician or student does not permit access to that same PHI in a research role)

Easiest mistake to make

- Ability to access PHI as a result of clinical duties is abused when it is used to access PHI for research purposes if IRB approval and HIPAA release mechanisms are not in place.
- Extracting PHI for research purposes requires
  - a CE workforce member assigned to perform that task by the CE
  - a Business Associate Agreement for non-workforce members.

More information

- IRB
- Online (researchers)
  - http://www.hpitp.buffalo.edu/hipaa/UB_HIPAA_ResearchHomePage.htm
- Online (UB formal policies/guidance)
  - http://www.hpitp.buffalo.edu/hipaa/Declarations_Positions.htm
- Centers for Medicare and Medicaid Services
  - http://www.cms.hhs.gov/HIPAAGenInfo/