HIPAA and Research at UB

Brian Murphy, MS

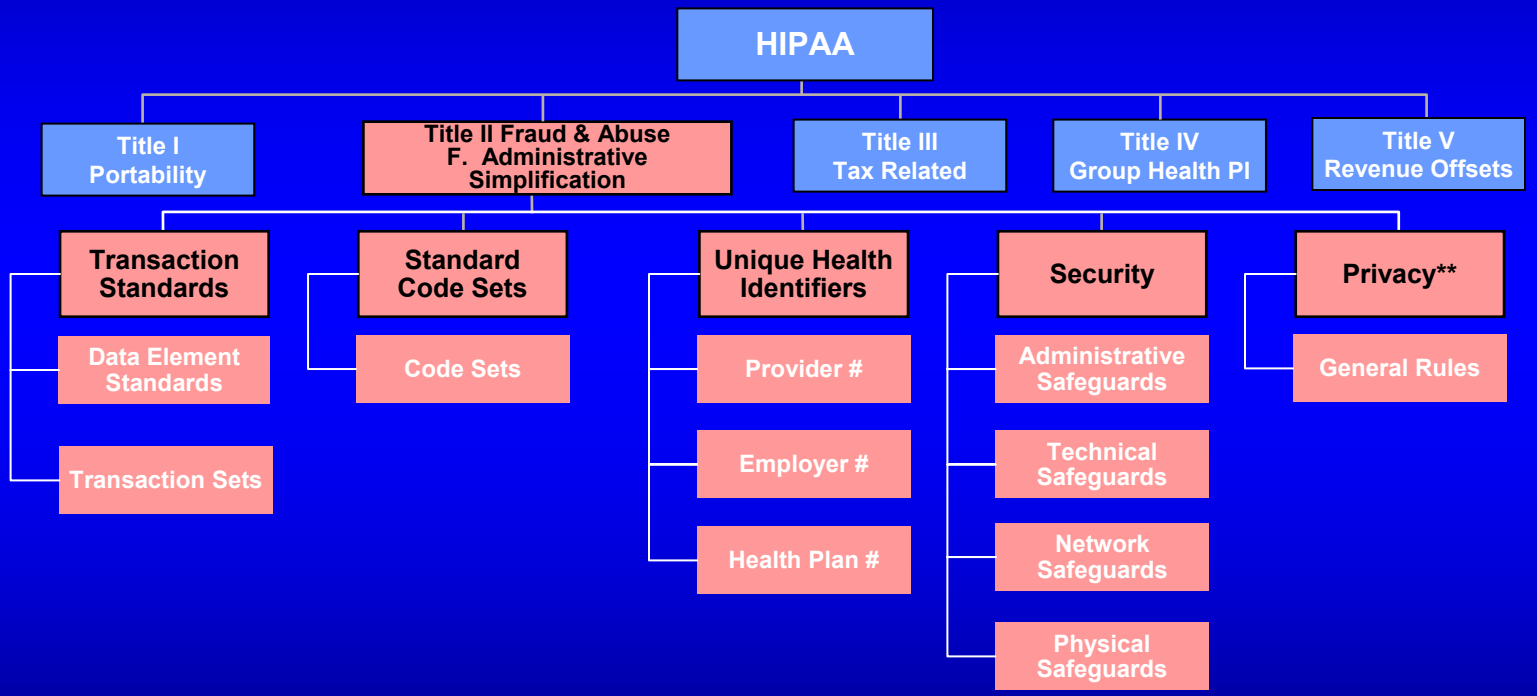
Director, University at Buffalo HIPAA Compliance *Office of the President*
Director, Health Professions IT Partnership *Office of the VP for Health Affairs*
bwmurphy@buffalo.edu

University at Buffalo
The State University of New York

Overview

- Elements of HIPAA
  - Covered and non-Covered Functions
- Privacy Rule & Research
  - PHI access mechanisms for research
  - Covered Function / IRB / Investigator responsibilities
  - HIPAA "obligations" for PHI held by researcher
  - Problems / solutions (some pending)

Elements of HIPAA



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
- **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: (est.. Spring 2005) National Provider Identifier (NPI)
  - Health Plan: (est. Spring 2005)

What is a covered entity?

- A health care plan
- A health care clearing house
- A health care provider *who engages in one of the HIPAA defined standard electronic transactions*

(1) Health care claims or equivalent encounter information.
(2) Health care payment and remittance advice.
(3) Coordination of benefits.
(4) Health care claim status.
(5) Enrollment and disenrollment in a health plan.
(6) Eligibility for a health plan.

(7) Health plan premium payments.
(8) Referral certification and authorization.
(9) First report of injury.
(10) Health claims attachments.
(11) Other transactions that the Secretary may prescribe by regulation."

Currently only 1-10 are in force.

HIPAA Administrative structure SUNY & UB

- SUNY is the hybrid entity
  - Privacy Officer: Steven Smith
  - Partnership with RF for research
- UB
  - Director, HIPAA compliance: Brian Murphy (2/03)
  - Unit HIPAA compliance coordinators
    - School of Dental Medicine: Mike Breene, CIO – HIPAA project manager (3/03)
- Medical and Dental Practice Plans
  - Privacy Officer: Tak Nobumoto (Spring 03)

Covered and non-Covered Functions

- HIPAA obligations
  - Covered entities and covered functions
    - Obligated to comply with all elements of HIPAA
  - Non-covered entities and functions
    - Obligated to obtain PHI from covered functions in HIPAA appropriate manner
- UB will only be declaring functions that provide health care ***and*** engage in HIPAA defined specific electronic transactions (or are health plans / clearinghouses) as covered functions
- UB adopting a 'HIPAA as best practices' approach to other elements of HIPAA

Function designations & Research

- Research done by UB faculty is 'owned' by the University and subject to UB HIPAA functional designations
- Outside of "UB designated covered functions", UB research will be considered a *non-covered* function.
  - If covered electronic transactions and healthcare occur as part of a research protocol within another covered entity, under these circumstances the (non-UB) covered entity portion of the research will be associated with that entity, i.e., with the individual/employer engaged in the covered electronic transactions associated with treatment (e.g., Practice Plan, Hospital)
  - All other aspects of research will occur in the (UB) non-covered function
  - At times CF and non-CF roles will be jointly held by a single individual. In these cases investigator must ensure that PHI flows from CF to non-CF research team in a HIPAA appropriate way

UB Covered Function Designations

- School of Dental Medicine
  - SDM has elected to place all of its operations within its covered function.
    - Patient Care, Education, Research
      - Research Centers
      - Individual Protocols
  - Aspects of RF HR associated with health plan administration

HIPAA Privacy Rule & Research

We're in the middle of the transition. Not all processes are set in stone or even at the final agreement stage … stay tuned

IIHI

§ 160.103 Individually Identifiable Health Information

- *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.

PHI

§ 160.501 Protected Health Information

- *Protected health information* 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

[§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]

Health Care Operations
[§164.501]

- *Health care operations* means any of the following activities of the covered entity to the extent that the activities are related to covered functions (subset listed…):
  - (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;

Health Care 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;

Health Care Operations (cont'd)

- (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
  - (6)(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.

Research under HIPAA

- *Research* means a systematic investigation including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. It is *not* part of TPO.
- Student 'research' exercises not designed "to develop or contribute to generalizable knowledge" are training activities and, as part of normal "Operations" under HIPAA, need not adhere to HIPAA research provisions

Covered function designation – how does it impact Research in a CF/NCF?

- Obtaining PHI for research
  - CF / NCF: Essentially no difference. Research falls outside of Treatment/Payment/Operations (TPO) within a CF and therefore PHI cannot be obtained from (or in) a CF for use in research unless it is obtained in a HIPAA appropriate way.
- Using PHI for research
  - CF: Must adhere to all HIPAA rules (including accounting for disclosures, BA agreements, protecting PHI, etc.); some benefits (reviews preparatory to research for recruitment, fewer disclosures requiring accounting); HIPAA liability for non-compliance
  - NCF: Adhere to HIPAA rules as "Best Practices"

Covered function designation – how does it impact Research in a CF/NCF?

- Redisclosure of PHI
  - CF: Not permitted except via HIPAA mechanisms; HIPAA liability for non-compliance
  - NCF: Specifically not permitted in some circumstances (e.g., BA / DUA contracts, waiver restrictions, etc.,); otherwise not permitted under HIPAA as "Best Practices" effort.
- Adhering to other aspects of HIPAA rules (T&C, Security, …)
  - CF: Mandatory; HIPAA liability for non-compliance
  - NCF: As "Best Practices"

Research transition provisions

- Prior to 4/14/2003
  - Signed informed consent obtained before 4/14/2003 will require no additional HIPAA documentation (re-consent after 4/14 will require HIPAA authorization or other HIPAA appropriate mechanism).
  - Studies granted waivers of informed consent before 4/14/2003 (IRB is in process of granting these now for appropriate exempted studies) will require no additional HIPAA documentation
- On and after 4/14/2003
  - HIPAA authorization *required* in addition to informed consents signed on or after 4/14/2003.
  - Studies granted waivers of informed consent *on or after* 4/14/2003 will be *required* to access IIHI by way of one of the HIPAA approved transfer mechanisms
  - All new protocols will be *required* to access IIHI by way of one of the HIPAA approved transfer mechanisms

Researcher access to PHI under HIPAA

- Reviews Preparatory to Research*
  - No information may be removed from covered entity
- Research on Decedents*
- Authorization
- De-identification
  - Requires a Business Associate Agreement with CE if de-identified dataset is created by a NCF UB researcher*
- Limited Dataset
  - Data Use Agreement
  - Usually requires a Business Associate Agreement with CE if creation of limited dataset is done by a NCF UB researcher*
- Waiver of Authorization*

*Covered entities required to account for these disclosures upon patient request.

Researcher access to PHI under HIPAA

- Reviews Preparatory to Research
- Research on Decedents
- Authorization
- De-identified data set
- Limited data set
- Waiver of Authorization

Reviews preparatory to research.

- The covered entity obtains from the researcher representations that:
  - (A) 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;
  - (B) No protected health information is be removed from the covered entity by the researcher in the course of the review; and
  - (C) The protected health information for which use or access is sought is necessary for the research purposes.

Reviews preparatory to research.

- No information collected with this mechanism may be removed from the covered entity
- Subject recruitment
  - Covered entity workforce member can use this mechanism to recruit subjects (OCR 12/2002 guidance)
  - Non covered entity workforce member *cannot* use this mechanism to recruit subjects (must use limited waiver; OCR 12/2002 guidance)
  - In either circumstance, recruitment activities should only be undertaken by providers who have a direct treatment relationship with the subject.

Reviews Preparatory to Research Workflow

- Researchers can download "Reviews Preparatory to Research" form from UB HIPAA Research web site
- Researchers should present completed document directly to covered entity in order to access PHI preparatory to research
- NB: "Preparatory to research" explicitly excludes actual conduct of research

Researcher access to PHI under HIPAA

- Reviews Preparatory to Research
- **Research on Decedents**
- Authorization
- De-identified data set
- Limited data set
- Waiver of Authorization

Research on decedent's information

- The covered entity obtains from the researcher:
  - (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.
- Subject to additional CE access policies

Research on Decedents Workflow

- Researchers can download "Research on Decedents" form from UB HIPAA Research web site
- Researchers should present completed document directly to covered entity in order to access decedent PHI
- CE may impose additional policy restrictions on access to such information

Researcher access to PHI under HIPAA

- Reviews Preparatory to Research
- Research on Decedents
- **Authorization**
- De-identified data set
- Limited data set
- Waiver of Authorization

Authorization

- Can be combined with informed consent (provided not for psychotherapy notes) or separate [§ 164.508(b)(3)(i)]
- Can condition the provision of research-related treatment on provision of an authorization for the use or disclosure of protected health information for such research [§ 164.508(b)(4)(i)]
- Should meet "minimum necessary" criteria (not required)
- A covered entity must document and retain any signed authorization under this section as required by §164.530(j). [§ 164.508(b)(6)]

Authorization

Core elements and requirements. [§ 164.508(c)(1)]

(i) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.

(ii) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.

(iii) The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure.

(iv) A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.

Authorization

Core elements and requirements. [§ 164.508(c)(1)]

(v) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research repository.

(vi) Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.

Authorization

Required Statements. [§ 164.508(c)(2)]

(i) The individual's right to revoke the authorization in writing, and either:

(A) The exceptions to the right to revoke and a description of how the individual may revoke the authorization; or

(B) To the extent that the information in paragraph (c)(2)(i)(A) of this section is included in the notice required by § 164.520, a reference to the covered entity's notice.

(ii) The ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either:

(A) The covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations in paragraph (b)(4) of this section applies; or

(B) The consequences to the individual of a refusal to sign the authorization when, in accordance with paragraph (b)(4) of this section, the covered entity can condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization.

(iii) The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer be protected by this subpart.

Authorization

Additional requirements. [§ 164.508(c)]

(3) *Plain language requirement.* The authorization must be written in plain language.

(4) *Copy to the individual.* If a covered entity seeks an authorization from an individual for a use or disclosure of protected health information, the covered entity must provide the individual with a copy of the signed authorization.

Authorization Workflow

- UB IRB will approve all authorization forms as part of research protocol submission
- Covered entities (KALEIDA Health, ECMC Healthcare Network, School of Dental Medicine) will rely on IRB determination of authorization's validity
- IRB will not approve an informed consent without also approving an associated authorization (and visa versa)

Authorization Workflow

- Approved authorizations must be signed by each research subject at time of subject enrollment
- Copy of signed authorization must be given to subject
- PI must deliver copy of signed authorization to CE (details vary by CE site)

Authorization
CE copy delivery (as of 4/3/2003)

- Original signed authorizations should be maintained by the PI. Copies of signed authorizations should be delivered by the PI to the CE:
  - **KALEIDA Health**: signed authorization forms must be delivered to the HIM site manager.
  - **ECMC Healthcare Network**: signed authorization forms should be sent to the ECMC HIPAA privacy officer, ECMC, 462 Grider Street Buffalo, NY 14215.
  - **School of Dental Medicine**: Please contact the SDM HIPAA project manager, Mike Breen, for SDM policy on this matter
  - **Other CEs**: contact CE for guidance
  - **UB Research not occurring in a covered entity/function**: no additional delivery of copies (other than to subjects) required

Researcher access to PHI under HIPAA

- Reviews Preparatory to Research
- Research on Decedents
- Authorization
- **De-identified data set**
- Limited data set
- Waiver of Authorization

De-Identified data set Workflow

- Affirm on IRB submitted PHI checklist that none of the listed information will be sought or used for purposes other than obtaining separate research data
- Affirm that, using information sought, the investigator 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. [§164.514(b)(2)(ii)]
- Obtain IRB "Certificate of De-Identification"

De-Identification Workflow

- Enter into CE BA agreement if NCF investigator will be performing de-identification (mechanism not yet developed)
  - NCF Investigator not permitted to possess any re-identification keys if de-identified data comes from a CF
  - For PHI not from CE, NCF investigator must ensure that re-identification keys are safely separated from de-identified PHI

Researcher access to PHI under HIPAA

- Reviews Preparatory to Research
- Research on Decedents
- Authorization
- De-identified data set
- **Limited data set**
- Waiver of Authorization

Limited Dataset [164.514](e)(1)

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 (similar to de-identified data set, but permits postal address information of town or city, state and zip; dates; other identifiers not explicitly prohibited)

- (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.

Researcher access to PHI under HIPAA

- Reviews Preparatory to Research
- Research on Decedents
- Authorization
- De-identified data set
- Limited data set
- Waiver of Authorization

Waiver of Authorization

- (ii) *Waiver criteria*. A statement that the IRB or privacy board has determined that the alteration or waiver, in whole or in part, of authorization satisfies the following criteria:
  - (A) The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements …

Waiver of Authorization waiver criteria (cont'd)

- (ii)(A)…
  - (1) An adequate plan to protect the identifiers from improper use and disclosure;
  - (2) An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
  - (3) Adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of protected health information would be permitted by this subpart;

Waiver of Authorization waiver criteria (cont'd)

- (ii)(B) The research could not practicably be conducted without the waiver or alteration; and
- (ii)(C) The research could not practicably be conducted without access to and use of the protected health information.

Waiver of Authorization waiver criteria IRB

- § 164.512(i)(1)(i) *Board approval of a waiver of authorization.* The covered entity obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization required by §164.508 for use or disclosure of protected health information has been approved by either:
  - (A) An Institutional Review Board (IRB), established in accordance with 7 CFR 1c.107, [references removed]; or
  - (B) A privacy board ….
- "in whole or in part" → IRB application of minimum necessary

Waiver of Authorization waiver criteria IRB (cont'd)

- (2) *Documentation of waiver approval*. For a use or disclosure to be permitted based on documentation of approval of an alteration or waiver, under paragraph (i)(1)(i) of this section, the documentation must include all of the following:

Waiver of Authorization waiver criteria IRB (cont'd)

- (i) *Identification and date of action*. A statement identifying the IRB or privacy board and the date on which the alteration or waiver of authorization was approved;
- (iii) *Protected health information needed.* A brief description of the protected health information for which use or access has been determined to be necessary by the IRB or privacy board has determined, pursuant to paragraph (i)(2)(ii)(C) [the research could not practicably be conducted…] of this section;

Waiver of Authorization waiver criteria IRB (cont'd)

- (iv) *Review and approval procedures.* A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures, as follows:
  - (A) An IRB must follow the requirements of the Common Rule, including the normal review procedures (7 CFR 1c.108(b)…[references removed]) or the expedited review procedures (7 CFR 1c.110…[references removed]);
- (v) *Required signature.* The documentation of the alteration or waiver of authorization must be signed by the chair or other member, as designated by the chair, of the IRB or the privacy board, as applicable.

Research PHI access mechanism responsibilities

- IRB responsibilities
  - Granting waivers of HIPAA authorization when appropriate
  - Validating HIPAA authorization forms
  - "De identification" certificates
  - Providing templates / worksheets / guidance for the above mechanisms as well as for reviews preparatory to research and research on decedents (http://www.hpitp.buffalo.edu/hipaa)
- CE responsibilities (SDM, Hospitals)
  - Ensure IIHI is not used or disclosed in a non-HIPAA manner
  - Account for disclosures of PHI (disclosure is to something 'outside of' the covered entity - not required for an authorization, de-identified dataset or limited dataset with DUA)
  - Reviews preparatory to research
  - Research on Decedents
- Mechanisms not yet determined
  - De-identification
  - Limited Dataset

Other issues

- Accounting for disclosures
- Designated Record Set
  - Patient right to review
  - Patient right to amend data
- BA / DUA signatories
- RF Contractual Language
- Delivering documentation to CEs/CFs
- HIPAA as “Best Practices” for NCFs

Accounting for disclosures

- *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.
  - Accounting for disclosures requires that covered entities provide individuals, upon request, with an accounting of all disclosures for the previous six years (or back to 4/14/2003)
  - A non-CE simply viewing PHI within a CE qualifies as a disclosure under the 'provision of access to' language

Research accounting for disclosures

- Required for research PHI disclosures occurring under the following HIPAA mechanisms:
  - Reviews preparatory to research
  - Research on decedents
  - Waiver of authorization
- *Not required* for research PHI disclosures occurring under the following HIPAA mechanisms:
  - Authorization
  - De-identified data set
  - Limited data set

Accounting for disclosures

- If the covered entity has made disclosures of PHI for a particular research purpose for 50 or more individuals, the accounting may, with respect to such disclosures for which PHI about the individual *may* have been included, provide:
  - (A) The name of the protocol or other research activity;
  - (B) A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;
  - (C) A brief description of the type of protected health information that was disclosed;
  - (D) The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;
  - (E) The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and
  - (F) A statement that the protected health information of the individual may or may not have been disclosed for a particular protocol or other research activity.

Accounting for disclosures

- If the covered entity provides an accounting for research disclosures in accordance with the '50 or more' provisions clause, and if it is reasonably likely that the protected health information of the individual was disclosed for such research protocol or activity, the covered entity shall, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.

Designated Record Set

- HIPAA gives patients rights to review/modify data held in the designated record set
- To avoid this problem, both CF and NCF researchers should not rely on data stored in a designated record set to comprise a portion of the research record set

Designated Record Set (cont'd)

Designated Record Set means:

- (1) A group of records maintained by or for a covered entity that is:
  - (i) The medical records and billing records about individuals maintained by or for a covered health care provider;
  - (ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
  - (iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals.
- (2) For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

Designated Record Set (cont'd)

- Restrictions to accessing DRS used in research
  - 164.524(a)(2)(iii): May be suspended for duration of research provided
    - Individual agreed to temporary suspension of this right as part of consent for research.
    - Right is restored upon completion of research
- HIPAA affords no access/modification rights to information not part of the DRS [164.526(a)(2)(ii & iii)
  - A Research Record Set that is maintained separate from the Designated Record Set would meet these criteria provided the research record set does not qualify as as part of the designated record set.

BA / DUA Contracts

- Will require signature other than investigator's
  - Likely a signature from RF for sponsored research
  - Mechanism for non sponsored research being investigated

RF Contractual Language
Research Sponsor access to PHI

- It is expected that Sponsor will receive information from Research Foundation project staff members in connection with or as a result of the RF's performance under this Agreement. Some of the information provided may be Individually Identifiable Health Information (IIHI) as defined in the Health Insurance Portability and Accountability Act (HIPAA) of 1996, and the regulations issued there under. Sponsor is hereby granted permission to receive and use IIHI provided by RF project staff members as allowed by the terms of this Agreement, in consideration of which Sponsor agrees to the following privacy provisions.

RF Contractual Language
Research Sponsor access to PHI

- Sponsor will use appropriate safeguards to prevent use or disclosure of IIHI other than as provided by this Agreement.
- Sponsor will not use or further disclose IIHI other than as required by law.
- Sponsor will report any unauthorized use or disclosure of IIHI that comes to Sponsor's attention to the RF.
- If Sponsor shares IIHI with third parties, Sponsor will assure that said third parties are subject to the same privacy obligations that are set forth in these provisions.
- Sponsor will provide access to IIHI in accordance with 45 CFR 524.

RF Contractual Language
Research Sponsor access to PHI

- Sponsor will make IIHI available for amendment, and incorporate amendments in accordance with 45 CFR 526.
- Sponsor will make information available to account for disclosures in accordance with 45 CFR 164.528.
- Sponsor will make its records regarding procedures and practices covering use and disclosure of IIHI available for purposes of determining Contractors compliance with these privacy provisions.
- At termination of this Agreement, Sponsor will, if feasible, return or destroy IIHI received from the RF and retain no copies thereof.
- It is understood and agreed that RF may terminate this Agreement if the RF determines that Sponsor is in material breech of the privacy provisions set forth above.

Delivery of material to CEs
IRB Responsibilities

- IRB will not approve a protocol involving the provision of health care or requiring access to PHI from a CE/CF until it has also approved the HIPAA mechanism for obtaining PHI (and visa versa)
- Notify CE of research protocols approved in the CE by the IRB on a monthly basis
- Provide CEs with copies of approved waivers of authorization

Research & UB's HIPAA "best practices" effort

- There are a number of units on campus that maintain IIHI and provide health care but are not part of UB's covered function
- Once the HIPAA mandatory covered functions are HIPAA compliant, efforts will be initiated to bring the non-mandatory units into a "best practices" compliance with HIPAA (efforts to start in ~Spring/Summer 2003)

Research & UB's HIPAA "best practices" effort

- Research at UB involving health care, whether or not within a covered function, will be required to follow the new IRB workflow model as part of an IRB QI initiative.
- Limit non-HIPAA liability that would arise for UB if privacy protections for research subjects were based on electronic transactions criteria
- Eliminate the need for prolonged analysis of covered function status with respect to individual protocols
- Other elements of HIPAA will be extended to research as part of UB's general HIPAA "best practices" initiative

Research Problems / Solutions
Disclosing PHI to a research sponsor

- Authorization (sponsor explicitly listed)
- De-identified data set
- Limited data set (sponsor explicitly listed in DUA)
- Waiver for "authorized oversight of the research study"
- As required by law
- Notes…
  - need to add RF "BA like" contract language
  - A "business associate" agreement is specifically NOT an appropriate mechanism for disclosure of PHI to research sponsors unless the sponsor is receiving PHI from the CE to provide a service to the CE. Minimum necessary limits PHI released to the sponsor to purposes of the service they are performing.

Research Problems / Solutions
PHI Database for future research

- Creation and maintenance of such a database is permitted under HIPAA
  - Must be explicitly stated in authorization if data is obtained via the authorization mechanism.
- Data in database cannot be used for future research until that new research has established its own HIPAA approved access mechanism for obtaining/using PHI
- Maintenance of a database for legitimate TPO purposes is permissible, and this database can be accessed for research purposes after that research has established its own HIPAA approved access mechanism for obtaining/using PHI

Research Problems / Solutions
Subject Recruitment

- Based on PHI from a CE/CF
  - *Cannot be undertaken* as an activity under 'reviews preparatory to research' if researcher is not part of CE/CF. In such cases a limited waiver will have to be sought.
  - Contact *only permitted* via health care provider with a primary treatment relationship to subject
- Direct recruitment (not based on knowledge of PHI from CE/CF)
  - permitted, but if PHI is collected as part of recruitment process by a researcher in a CF, it becomes PHI that is subsequently protected under HIPAA.

Additional Resources

- UB HIPAA WEB site
  - http://www.hpitp.buffalo.edu/hipaa
- UB HIPAA Research WEB site
  - UB/HHS/OCR FAQs; OCR HIPAA Research Guidance; Definitions; downloadable forms, templates, worksheets for use with IRB and CEs/CFs, IRB memos, RF links
  - http://www.hpitp.buffalo.edu/hipaa/UB_HIPAA_ResearchHomePage.htm