September, 2006
HIPAA at UB
Senior Management Orientation

Brian Murphy

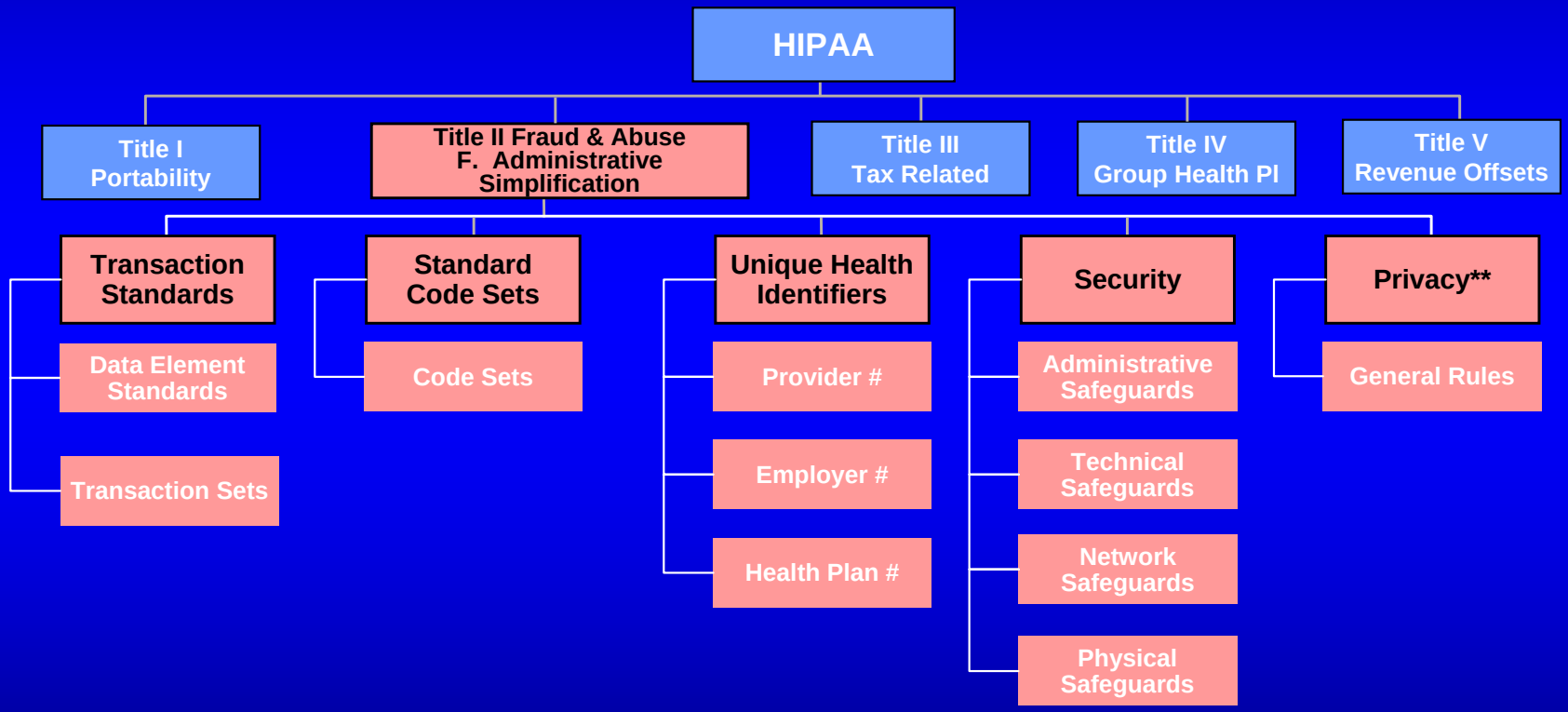
UB Director of HIPAA Compliance

bwmurphy@buffalo.edu

What is HIPAA

- Congress
  - Public Law 104-191; August 21, 1996 "Health Insurance Portability and Accountability Act of 1996"
- Dept of Health and Human Services (DHHS)
  - Multiple sets of regulations implementing various components of HIPAA

Background: HIPAA has many parts



Title II, Subtitle F - Rationale

"It is the purpose of this subtitle to **improve** the Medicare program under title XVIII of the Social Security Act, the medicaid program under title XIX of such Act, and **the efficiency and effectiveness of the health care system, by encouraging the development of a health information system through the establishment of standards and requirements for the electronic transmission of certain health information**."

Title II, Subtitle F - Enforcement

- DHHS Centers for Medicare and Medicaid Services
  - Transactions & Codesets
  - Security
  - Identifiers
- DHHS Office of Civil Rights
  - Privacy
- Department of Justice
  - Criminal Penalties

Title II, Subtitle F - Triggers

- Complaints by individuals
- Accrediting bodies utilizing ‘whistleblower’ provisions of HIPAA
- DHHS Office of Inspector General (2005 Audit)
  - CE Compliance with Privacy Rule
  - Assess College and University policies and procedures for protecting the privacy of medical records of persons participating in NIH-funded clinical trials and other research

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” relative to their interactions with CEs

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

Health Care Provider

§ 160.103: 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

§ 160.103: 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.

UB Covered Entities / Functions

- SUNY Hybrid Entity
  - SUNY Administration based HIPAA Privacy and Security Officers
  - SUNY-UB
    - Campus liaison to SUNY – UB Director of HIPAA Compliance
    - Covered Function: School of Dental Medicine clinic / academic operations
      - Mike Breene, SDM CIO and HIPAA project manager
- NON-SUNY
  - Research Foundation: personnel activities related to its Health Plan
    - Susan Steck, Director, RF HR Services
  - Clinical practice plans associated with the Medical School
    - Tak Nobumoto Security/Privacy officer
  - Clinical practice plans associated with the Dental School
    - Jim Harris Security/Privacy officer
  - Individual faculty who are health care providers in roles not related to SUNY activities (physical therapists, social workers, nurses, pharmacists, etc.)

UB *non-HIPAA* Functions associated with healthcare or health related information

Treatment and/or research without qualifying electronic transactions

- Research Institute On Addictions
- Division of Athletics
- Dept. of Psychology
  - Psychological Services Center
  - Motor Vehicle Accident Clinic
  - Center for Anxiety Research
  - Center for Children and Families
  - Depression Research and Treatment Program
  - Laboratory for Study of Individual Differences and Substance Use
- Student Affairs
  - Student Counseling Services
  - Student Health Services
  - Sub Board I Pharmacy

Health Information and/or research but no treatment or other HIPAA qualifying function

- Uniform Data Systems for Medical Rehabilitation (UDSMR)
- UBF / UBFA / UBFS
- UB HR related
  - Disability Services
  - Workers Compensation
  - Employee Assistance Program
- University Medical Resident Services
- University Dental Resident Services
- Schools
  - RPCI Graduate division of UB
  - Social Work
  - Medicine and Biomedical Sciences
  - Nursing
  - Pharmacy
  - Public Health and Health Professions
- Institutional Review Board
  - Adverse Event Reporting

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)

Protected Health Information

[Privacy: 45 CFR §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 BAC in place]

Consequences of violating HIPAA

- Civil & Monetary Penalties
  - $100/"person"/specific violation
    - Max $25,000 per specific violation/year
    - Privacy: 56 standards, 58 implementation specifications
    - Security: 18 standards, 42 implementation specifications
- Criminal Penalties
  - 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
- Civil suits citing HIPAA as a reaonable 'norm'
- Employer sanctions (some form of sanction required by HIPAA)

Ongoing UB HIPAA obligations

- Maintain accurate and current list of Covered Entities on campus
  - Units must self-report changes in status to UB Director of HIPAA compliance
- Maintain documentation related to HIPAA policy/practice decisions
- Reporting to SUNY Administration
  - Changes in SUNY covered entity list
  - Annual Privacy and Security self-audit
  - HIPAA violations within covered entities

Ongoing UB HIPAA obligations

- Compliance with HIPAA in covered entities
- Appropriately manage HIPAA related contractual documents
  - Business Associate Contracts/Agreements
  - Limited Data Sets / Data Use Agreements
  - *MUST* be reviewed for appropriateness and approved by UB Director of HIPAA compliance and appropriate counsel (SUNY, UBF, RF, etc.)
  - Signature authority has not been delegated for HIPAA related agreements

Ongoing UB HIPAA obligations

- Students
  - Educate students on general principles of HIPAA if part of their educational experience occurs within a CE
  - Also requires a SUNY clinical affiliation agreement (distinct from hospital affiliation agreements) if this experience is part of their degree requirement
- Researchers
  - Ensure UB researchers are not exposing CEs to HIPAA liabilities by inappropriately acquiring research data

Voluntary UB obligations?

- Implement best-practices provisions of HIPAA for health information that does not fall under HIPAA
  - Currently individual choice of unit as to what type of protections are deployed
- NB: NY Disclosure Law

HIPAA and Research

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)

Accessing Information

- Protected Health Information in a CE can be accessed for research purposes, by someone within or outside of the CE, only by one of seven mechanisms prescribed by HIPAA.
- The ability to access information as a consequence of treatment responsibilities is *not* one of these mechanisms.
  - Inappropriate access creates liability for covered entities under HIPAA civil/monetary penalties.

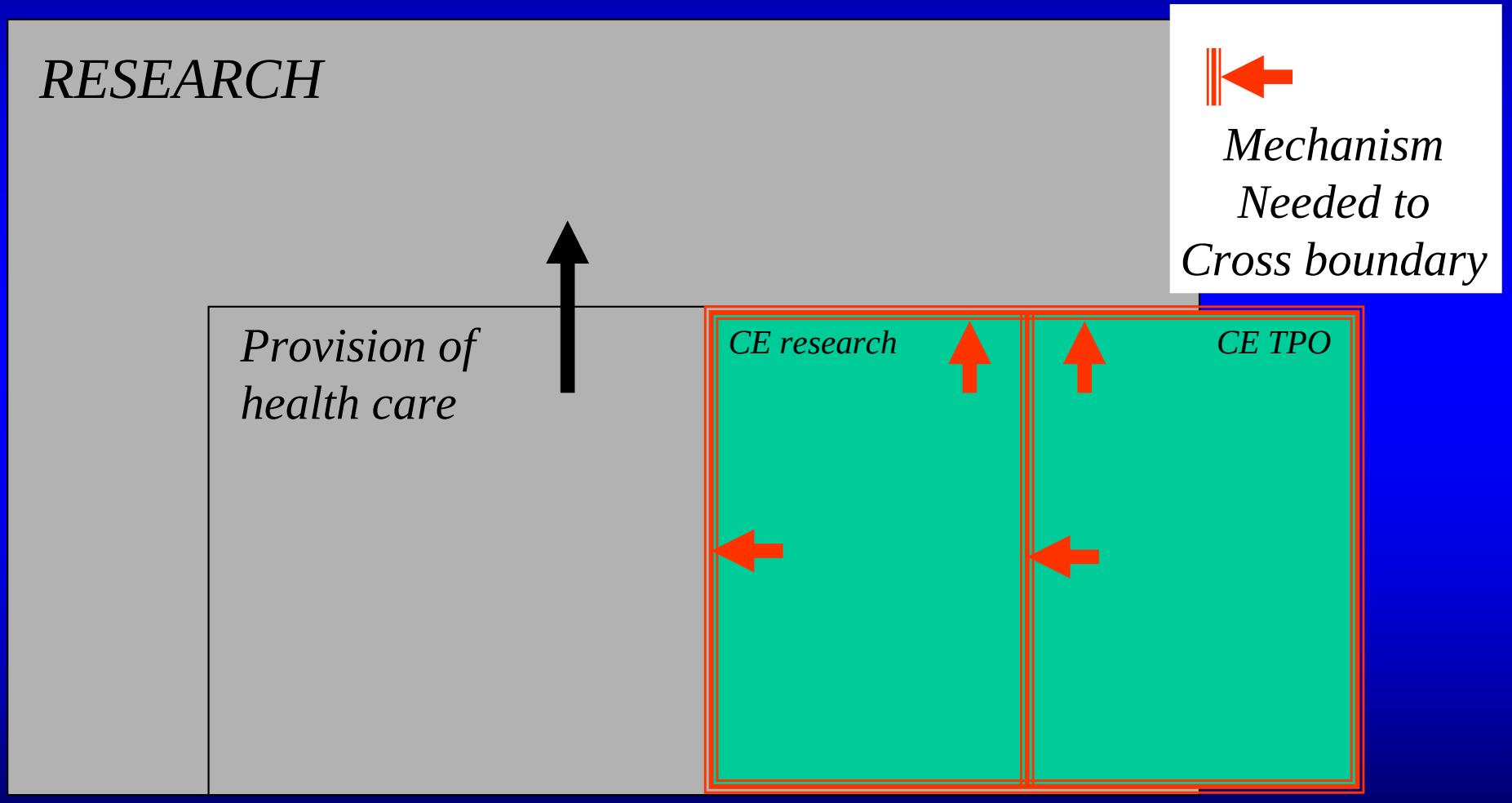
Removing UB research function from UB, SUNY and 3rd party CEs

- UB is part of the SUNY Hybrid Covered Entity under SUNY
- 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 or hospital activity
- UB has *defined* its research activity as not being part of any UB/SUNY covered function

UB Research, Treatment, HIPAA

- UB Research and UB or 3rd party CE Treatment may occur simultaneously
- Research can only access information via one of the seven mechanisms prescribed by HIPAA
- Information in the possession of a researcher obtained through one of those mechanisms is no longer protected by HIPAA (unless contractually via the mechanism)
- Treatment information in the possession of a CE health care provider remains protected by HIPAA
- Researcher and Clinician *may* be the same person but research and clinical data must *always* be segregated

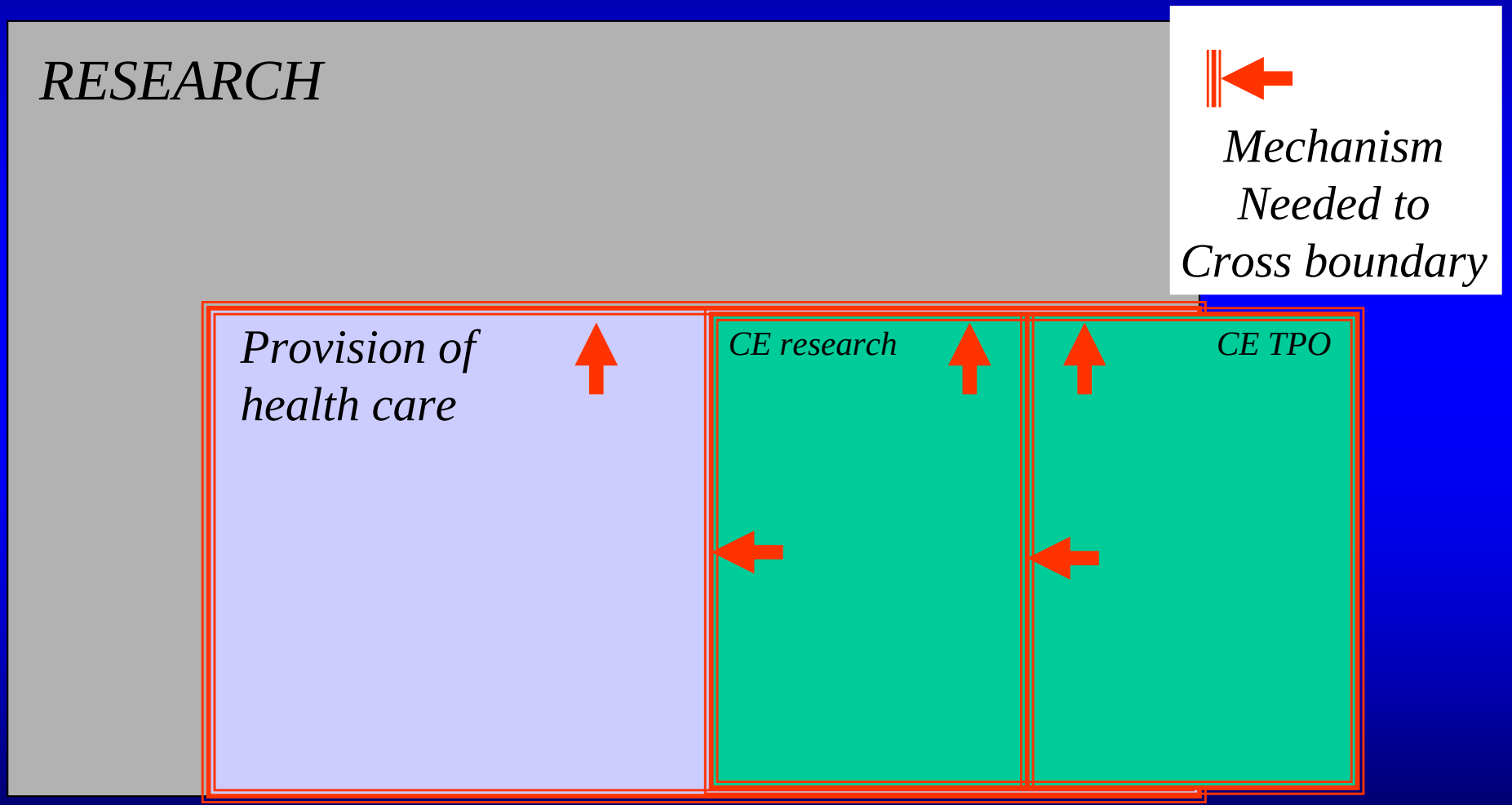
HIPAA Boundaries requiring release mechanisms for research use of PHI



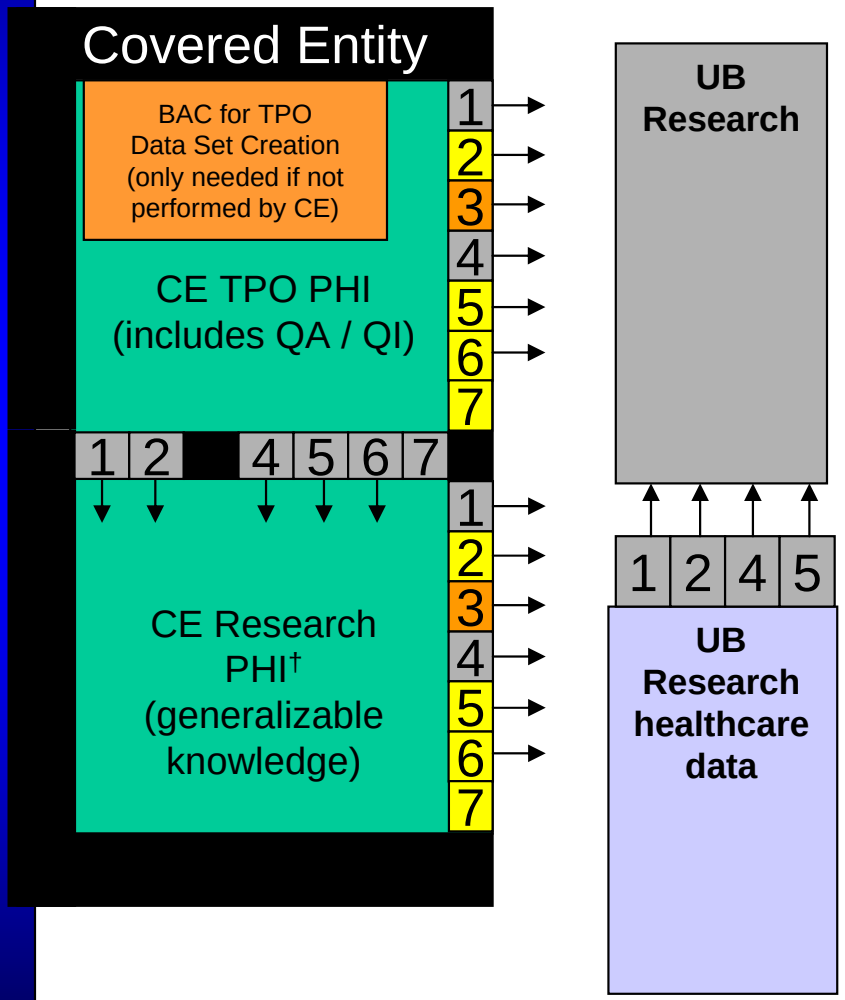
HIPAA + local (UB) Policy

- UB extends HIPAA's requirement for a release mechanism to all research protocols performed by UB researchers *involving the provision of healthcare* so that the same kind of information does not receive different protections based solely on where it came from.
  - Direct recommendation of Ms. Julie Kaneshiro, Policy Team Leader in the Office for Human Research Protections (OHRP), Division of Policy and Assurances, U.S. Department of Health and Human Services (DHHS).
  - eliminates need for IRB to engage in 'is there a CE involved?' analysis for each protocol.

UB IRB Boundaries requiring release mechanisms for research use of PHI



HIPAA + UB Policy 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 Path for Investigators

- IRB reviews protocols
- If health care and identifiable 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 releasing information to UB researchers
  - Common forms developed for UB/ECMC/Kaleida

HIPAA Path for Investigators

- Business Associate Agreements
  - Required with a covered entity if investigator extracting information from a covered entity is not part of the covered entity's workforce.
  - Covered Entity to Employer (source of W2) contractual agreement which must be negotiated on a case by case basis
    - SUNY / UBFA / RF

Research: CE Burdens

- Ensure information is released to researchers only through one of the HIPAA permitted mechanisms
- Account for disclosures of information, when required by HIPAA
  - Patients may request an accounting of such disclosures, and CE is mandated to provide it under HIPAA

WHAT DOES THE PRIVACY RULE REQUIRE FROM COVERED ENTITIES?

	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

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/