
[B3] How IRBs are Implementing HIPAA: Finding the Best Fit for Your Institution

*The 18th Annual Meeting of the Applied Research
Ethics National Association*



December 5, 2003
Washington DC

Faculty



- John Falletta, MD
 - Duke University Health System
 - Pediatric Hematologist/Oncologist, Senior IRB Chair
- Tammy Sayers Lesko
 - The Copernicus Group IRB
 - Director of Quality Assurance & Regulatory Compliance
- Brian Murphy, MS
 - State University of New York at Buffalo
 - Director, HIPAA Compliance

Agenda

- HIPAA in Research
- 7 PHI Access Keys for Research and Points to Consider
- Institutional “Fit”
 - DUHS
 - CGIRB
 - SUNY at Buffalo
- HIPAA and the Common Rule
- Questions & Answers



Who does HIPAA Apply to?

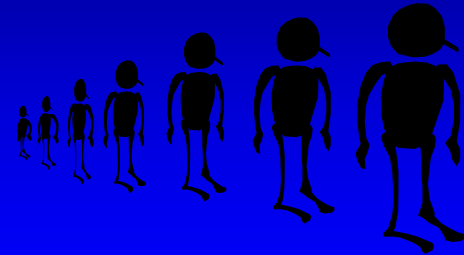
- Covered entities

- Health Care Plans;

- Health Care Clearinghouses;

- Health Care Providers who engage in specific electronic transactions.

- Also may include operations designated as part of the “Health Care Component” within a hybrid entity.



HI

Health Information

- Any information in any form or medium (oral, written, recorded).
- Information created or received by health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse.



HI

Health Information (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.



IIHI

Individually Identifiable Health Information

- Is HI (excluding that created by a public health authority, school or university, or life insurer) that:
 - Is created or received by a health care provider, health plan, employer, or health care clearinghouse
 - Identifies the individual or there is a reasonable basis to believe the individual can be identified



PHI

Protected Health Information



- PHI that is transmitted or maintained in any medium
- Excludes:
 - Education records covered by the Family Educational Rights and Privacy Act.
 - Employment records held by a covered entity in its role as employer.
 - Records of student \geq age 18 attending postsecondary education made or maintained by health care provider and used to provide treatment to student and not available to anyone other than those providing treatment or health care provider of student's choice.

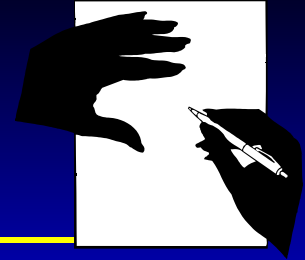
Protected Health Information

- HIPAA specifically recognizes that PHI may be created, used and disclosed in the course of performing research.



PHI

Summary



- Any information in any form or medium (oral, written, recorded).
 - Transmitted or maintained in any medium.
 - Created by a health care provider (some exclusions in educational settings), health plan or health care clearinghouse.
 - 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.
 - HIPAA protections apply to PHI created or received by a covered entity.
-



Protected Health Information

Points to Consider



- You can't identify PHI by looking at it – you also have to know where it comes from.
 - It isn't PHI if it doesn't come from a covered entity.
- A static piece of information can alternate between being PHI and non-PHI as it transits covered entities and non-covered entities.
 - Even within a covered entity, PHI that becomes part of employment records is no longer PHI.

Items Defined as Identifiers (1-10)

- Names
- Addresses /ZIP codes*
- Dates except year
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical Record Numbers
- Health plan beneficiary numbers
- Account numbers



Items Defined as Identifiers (11-18)

- Certificate/license numbers
- Vehicle identifiers and serial numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers
- Full face photographic images
- **Any other unique identifying number, characteristic or code**



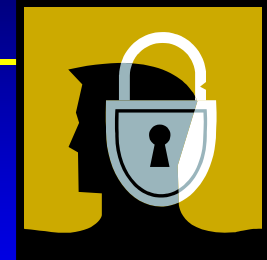
What does HIPAA protect?

- 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)



The “Why” of the Privacy Rule

<http://www.hhs.gov/ocr/hipaa/finalmaster.html>



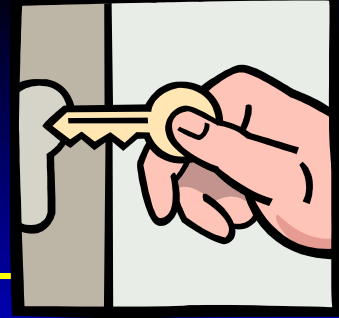
The Privacy Rule for the first time creates national standards to protect individuals' medical records and other personal health information.

- It gives patients more control over their health information.
- It sets boundaries on the use and release of health records.
- It establishes appropriate safeguards that health care providers and others must achieve to protect the privacy of health information.
- It holds violators accountable, with civil and criminal penalties that can be imposed if they violate patients' privacy rights.
- And it strikes a balance when public responsibility requires disclosure of some forms of data - for example, to protect public health.



December 5, 2003
Washington DC

Privacy Rule: Advantages to Patients



- For patients - it means being able to make informed choices when seeking care and reimbursement for care based on how personal health information may be used.
 - It enables patients to find out how their information may be used and what disclosures of their information have been made.
 - It generally limits release of information to the minimum reasonably needed for the purpose of the disclosure.
 - It gives patients the right to examine and obtain a copy of their own health records and request corrections.

Impact of HIPAA

- Does *not* reduce the effect of the Common Rule or FDA regulations.
- Mandates more protections to ensure privacy of subjects and confidentiality of data.
- Requires action whenever any PHI is used for research.



HIPAA PHI and Research



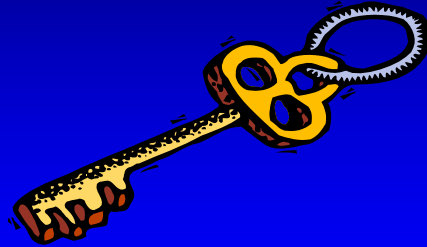
- HIPAA provides 7 “keys” to accessing PHI.
- Keys permit PHI to move from covered entity treatment side to researchers.
- Implementation of some keys and activities related to them is dependent on whether researcher is within the covered entity holding the PHI.



Research Access to PHI

- **Authorization**

45 CFR §164.508

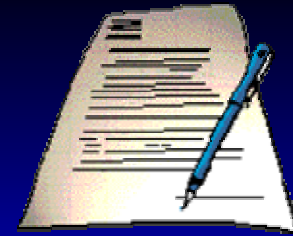


- Waiver or Alteration of Authorization
- Review Preparatory to Research
- Research on Decedents
- Transition Provisions
- De-identified Data
- Limited Data Set



December 5, 2003
Washington DC

Authorization



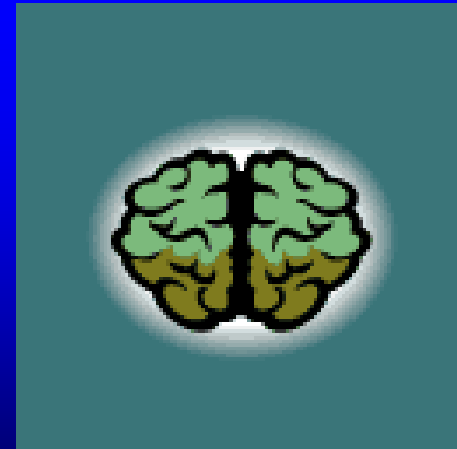
- Authorization specific to disclosure required for external research (cannot be “open ended” for unspecified future research).
 - Multiple specific implementation requirements (see handouts).
 - May be a stand alone document or combined with the informed consent document.
 - Revocation right balanced with ‘Reliance exception’.
 - Disclosures not subject to “accounting for disclosures”.
-



Authorization

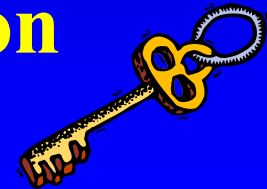
Points to Consider

- To combine or not combine with Informed Consent Form.
- Ensuring a complete listing of recipients.
- State law pre-emption.



Research Access to PHI

- Authorization
- **Waiver or Alteration of Authorization**
45 CFR §164.512(i)(1)(i) & §164.512(i)(2)
- Review Preparatory to Research
- Research on Decedents
- Transition Provisions
- De-identified Data
- Limited Data Set



Waiver of Authorization

- (1) *Permitted uses and disclosures.* A covered entity may use or disclose protected health information for research, regardless of the source of funding of the research, provided that:
 - (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 ...
 - (B) A privacy board that:



Waiver Requirements

- (i) *Identification and date of action.*
- (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:



Waiver Requirements (2)

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



Waiver Requirements (3)

- (A) ... involves no more than a minimal risk to the privacy of individuals , based on, at least, the presence of the following elements:
 - (A)(1) An adequate plan to protect the identifiers from improper use and disclosure;
 - (A)(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



Waiver Requirements (4)

- (A)(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 Requirements (5)

- (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) of this section;
- (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:



Waiver Requirements (6)

- (iv)(A) An IRB must follow the requirements of the Common Rule, including the normal review procedures or the expedited review procedures
- (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.



Waiver or Alteration of Authorization

Points to Consider

- Define “practicable”.
- Institutional Policy: whose waiver is acceptable?
- What is an “alteration” in whole or in part?
- What is a “partial waiver”?
- IRB or Privacy Board?



Privacy Board Composition

- (1) Has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests;
 - (2) Includes at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities; and
 - (3) Does not have any member participating in a review of any project in which the member has a conflict of interest.
-



Privacy Board Review Procedures

- (B) A privacy board must review the proposed research at convened meetings at which a majority of the privacy board members are present, including at least one member who satisfies the criterion stated in paragraph (i)(1)(i)(B)(2) of this section, and the alteration or waiver of authorization must be approved by the majority of the privacy board members present at the meeting, unless the privacy board elects to use an expedited review procedure in accordance with paragraph (i)(2)(iv)(C) of this section;



Privacy Board Review Procedures (2)

- (C) A privacy board may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the individuals who are the subject of the protected health information for which use or disclosure is being sought. If the privacy board elects to use an expedited review procedure, the review and approval of the alteration or waiver of authorization may be carried out by the chair of the privacy board, or by one or more members of the privacy board as designated by the chair.



Research Access to PHI

- Authorization
- Waiver or Alteration of Authorization
- **Review Preparatory to Research**
 - 45 CFR §164.512(i)(1)(ii)
- Research on Decedents
- Transition Provisions
- De-identified Data
- Limited Data Set



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 to 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

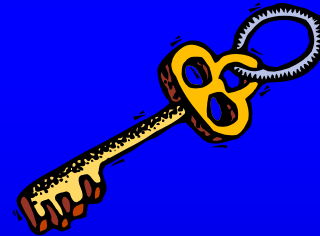
Points to Consider

- Can information acquired in this phase be used for subsequent research purposes?
- OCR Guidance with respect to this mechanism and subject recruitment
 - Researcher within CE holding PHI
 - Researcher outside of CE holding PHI
- How will the covered entity document researcher “representations”?



Research Access to PHI

- Authorization
- Waiver or Alteration of Authorization
- Review Preparatory to Research
- **Research on Decedents**
 - 45 CFR §164.512(i)(1)(iii)
- Transition Provisions
- De-identified Data
- Limited Data Set



Definition of “Human Subject”

Operational Change due to HIPAA

An ~~living~~ individual about whom an investigator...conducting research obtains (1) data through intervention or interaction with the individual, or (2) identifiable private information.



Research on Decedents

- 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.



Research on Decedents

Points to Consider

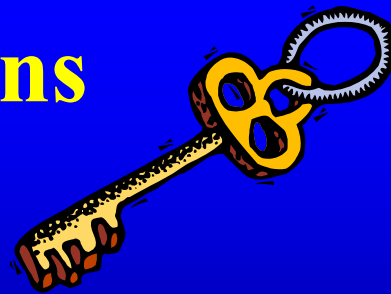


- It is up to the covered entity whether proof of death is required.
- How will covered entity document researcher “representations”?
- Sometimes decedent PHI involves the living (household members, e.g., in decedent record held by hospice who considers those folks also under hospice care).



Research Access to PHI

- Authorization
- Waiver or Alteration of Authorization
- Review Preparatory to Research
- Research on Decedents
- **Transition Provisions**
 - 45 CFR §164.532(c)
- De-identified Data
- Limited Data Set



Transition Provisions (“Grandfathering”)

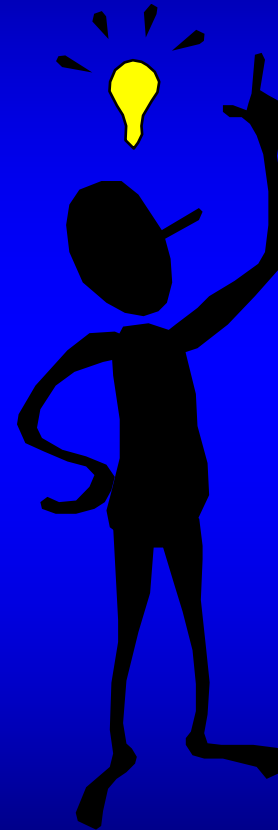
- Permits the use and disclosure of PHI created or received before or after April 14, 2003 if one of the following was obtained prior to that date:
 - An authorization or other express legal permission from an individual to use or disclose protected health information for the research;
 - The informed consent of the individual to participate in the research; or
 - A waiver, by an IRB, of informed consent.
- **If subjects must be re-consented, there must be an authorization or waiver in place.**



Transition Provisions

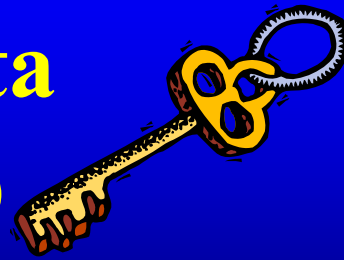
Points to Consider

- IRB 'exempted' studies not grandfathered.
- Obtaining knowledge of “agreed-to restrictions”.



Research Access to PHI

- Authorization
- Waiver or Alteration of Authorization
- Review Preparatory to Research
- Research on Decedents
- Transition Provisions
- **De-identified Data**
45 CFR §164.514(a-c)
- Limited Data Set



De-identified Data Set

- Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.



De-identified Data Set (2)

- A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable 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 documents the methods and results of the analysis that justify such determination;



De-identified Data Set (3)

- Removal of 18 (currently) identifiers of the individual or of relatives, employers, or household members of the individual.
- 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 Data Set (4)

- 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.



Anonymization vs. HIPAA De-identification

The only setting where IRB approval of anonymization (unlinking) does not also confer approval of HIPAA de-identification is when the anonymized (unlinked) health information contains an event date more specific than the year, or a geocode more specific than State or 3 digit zip code, or a subject's specific age if over 89 years (instead state as 90+ years).



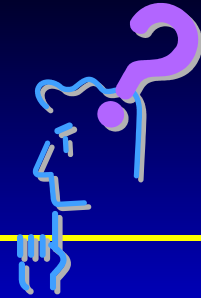
HIPAA De-identification vs. Anonymization

The only setting where IRB approval of HIPAA de-identification does not also confer approval of anonymization (unlinking) is when a code with a key linking back to the subject is retained with the de-identified data.



De-identified Data Set

Points to Consider

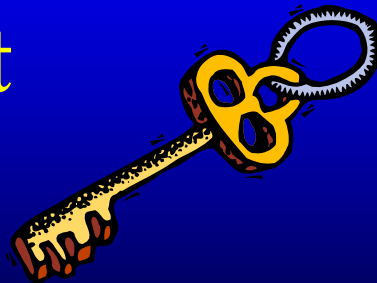


- Creation of de-identified data set is an activity of the covered entity; may require business associate agreement for outside researcher to create data set.
- If researchers are outside of the covered entity, “Re-identification” mechanism may be cumbersome or non-existent (preventing potential mandated follow-up).

Research Access to PHI

- Authorization
- Waiver or Alteration of Authorization
- Review Preparatory to Research
- Research on Decedents
- Transition Provisions
- De-identified Data
- **Limited Data Set**

45 CFR §164.514(e)



Limited Data Set

- A limited data set (LDS) is protected health information that excludes the same identifiers as a de-identified data set except for the following (which may appear in a LDS):
 - Town or city, state, and zip code
 - Dates
 - Any other unique identifying number, characteristic or code (except those explicitly prohibited)



Limited Data Set (2)

- A covered entity may use or disclose a limited data set LDS for research purposes if the covered entity enters into a *data use agreement* (DUA) with the limited data set recipient.



Data Use Agreement

- Required in order to obtain a LDS for research purposes.
- Establishes permitted uses and disclosures of the LDS.
- May not authorize the LDS recipient to use or further disclose PHI in any manner not available to a covered entity.
- Establish who is permitted to use or receive the LDS.



Data Use Agreement (2)

- Provides that the limited data set recipient will:
 - Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;
 - Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;
 - Report to the covered entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;
-

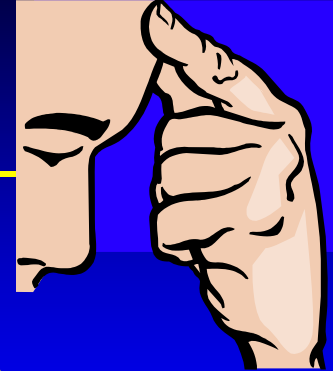


Data Use Agreement (3)

- Ensure that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information;
- **Do Not identify the information or contact the individuals.**



Limited Data Set Points to Consider



- Creation of LDS (an activity of the covered entity; may require a Business Associate Agreement and possibly a waiver of authorization for screening purposes if done by outside researcher).

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

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



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 (2)

- (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.
-



BREAK

We will reconvene in 15 minutes



December 5, 2003
Washington DC

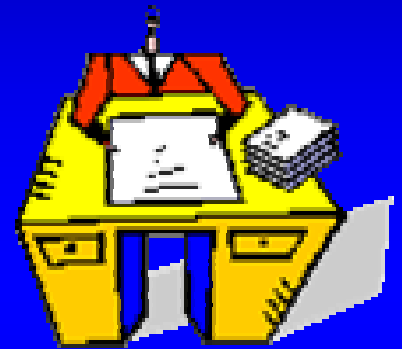
Ascertainment & Recruitment

- Treatment provider may discuss with **patient**.
- Patient initiated contact with researcher.
- Waiver of Authorization from IRB permitting discussion with researcher.
- Researcher posts flyers and advertises.



Ascertainment/Recruitment Process

If PHI or other identifiable private information is to be recorded by a member of the covered entity during the ascertainment/recruitment process, consent of the potential subject, or IRB approval of a Waiver of Consent, must be obtained.



(DHHS NIH guidance issued in 08/03 - FAQ on page 10)
http://privacyruleandresearch.nih.gov/pdf/IRB_Factsheet.pdf



December 5, 2003
Washington DC

IRB Responsibilities under HIPAA

- Formal IRB (or Privacy Board) responsibility only for granting alterations to, or waivers of, authorization requirement.
- Policy decisions have IRBs and/or Privacy Boards taking on additional responsibilities with respect to other 6 keys.
- Privacy Boards cannot fulfill Common Rule provisions. Common Rule provisions can only be met by IRBs.



Training of IRB and Investigators



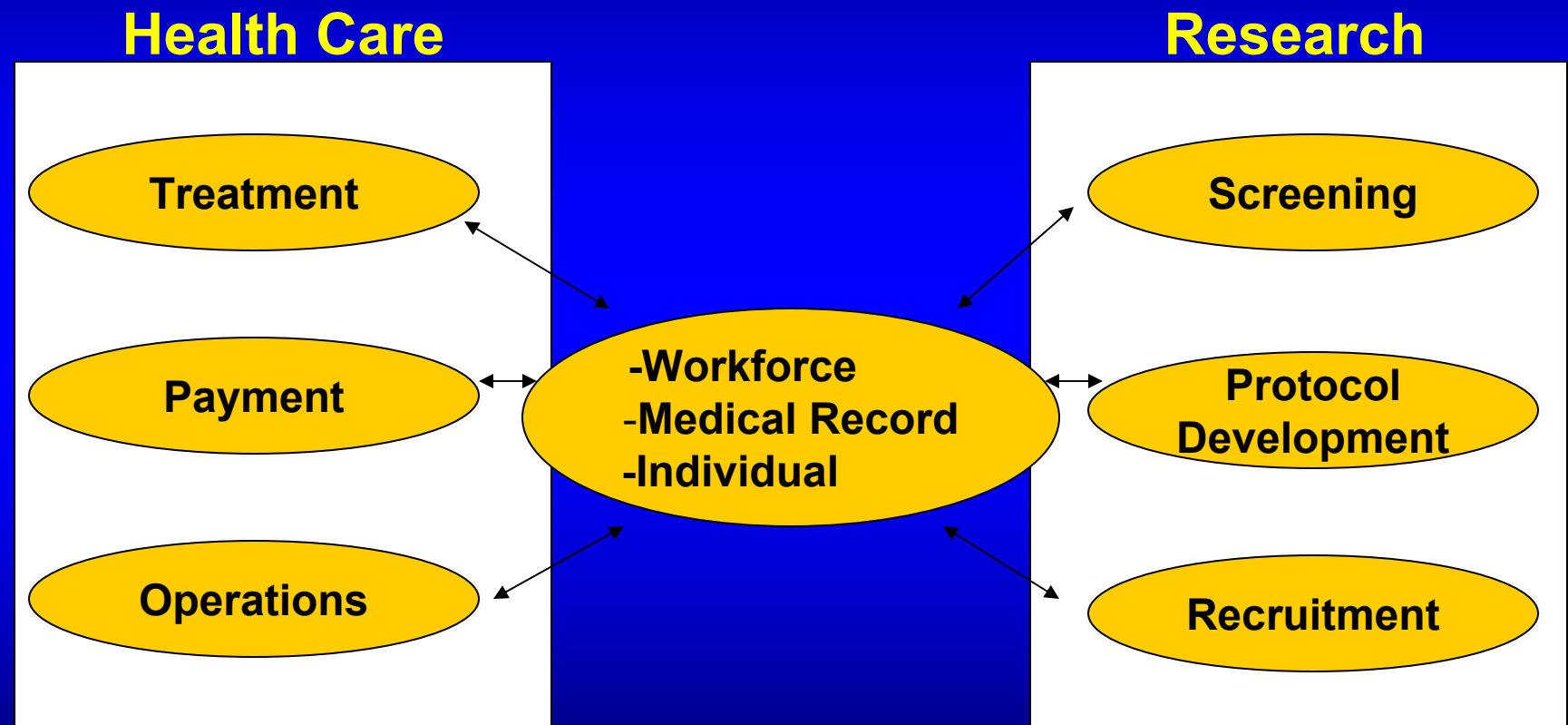
- IRB Training
 - Requirements of the Privacy Rule
 - Policies and Procedures of Company/Institution
- Training will assist in the Board being able to make their decisions.
- Make sure all members are informed when unique situations arise for consistency and future reference.
- Investigator Training
 - Requirements of the Privacy Rule
 - Policies and Procedures of Company/Institution
- Providing guidance and information to the Investigator will assist him/her in making proper submissions to the IRB.
- This will also aid in his/her proper implementation of procedures.

HIPAA Implementation

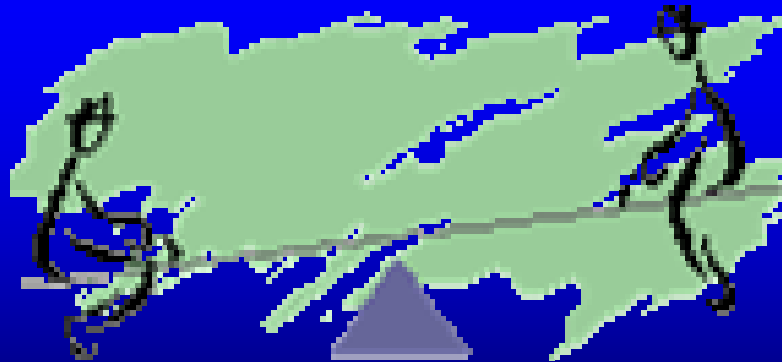


- HIPAA regulations provide flexibility.
- Implementation at a particular institution, and subsequent involvement of the IRB, depend upon
 - HIPAA regulations;
 - State Law (requisite pre-emption analysis);
 - Individual IRB/Institution policies aimed at simplifying the job of following the regulations;
 - Interpreting regulations and “guidance”
 - Workflow between covered and non-covered entities.

Recognizing The Overlap of PHI

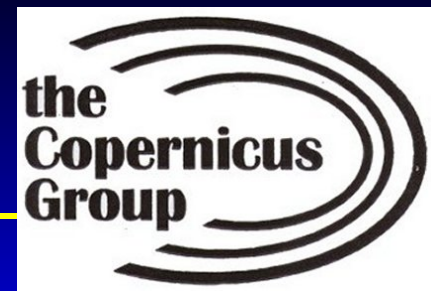


Comparison of each IRB Institutional “Fit”



December 5, 2003
Washington DC

Copernicus Group IRB HIPAA Implementation

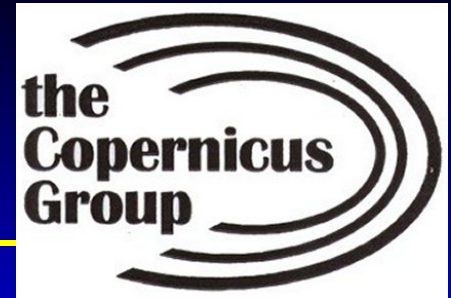


- CGIRB is an independent IRB.
 - Not a covered entity or business associate.
- CGIRB created a HIPAA subcommittee, composed of Board and Staff Members to evaluate our HIPAA policies and procedures.
- CGIRB is not a Privacy Board and is not affiliated with one.



December 5, 2003
Washington DC

Copernicus Group IRB HIPAA Implementation (2)



- All HIPAA Authorization forms and waivers/alterations of authorization for research, where CGIRB is the IRB of record, must be IRB reviewed and approved prior to use.
- CGIRB has a standard HIPAA Authorization form that includes all required elements.
- CGIRB provided site-specific, study-specific HIPAA Authorization forms for all sites who were actively enrolling on April 14, 2003.
- CGIRB continues to reassess our policies and procedures.



December 5, 2003
Washington DC

State University of New York

- SUNY – 64 campus hybrid entity
 - Upstate Medical University, Syracuse NY
 - Academic Medical Center, research within HIPAA covered function
 - University at Buffalo, Buffalo NY
 - Academic Medical Center, research outside of HIPAA covered function
- Individual campuses (64) to determine their covered functions.
- System guidance provided with respect to research “the matrix” ...



SUNY Guidance Matrix

RESEARCH

<p>Conduct One of the Standard Electronic Transactions ?</p> <p>No</p> <p>Yes</p>		<p>HIPAA Compliance Strongly Recommended</p>		<p>Not Required to Comply with HIPAA</p>
		<p>Not Covered by HIPAA (Not Legally Subject to HIPAA -)</p>	<p>Not Covered by HIPAA</p>	
<p>Required to comply with the requirements of HIPAA</p>		<p>Protected Health Information (Covered by HIPAA)</p>	<p>Not Covered by HIPAA</p>	<p>Not Required to Comply with HIPAA</p>
		<p>Yes</p>	<p>Individually Identifiable Health Information?</p>	



December 5, 2003
Washington DC

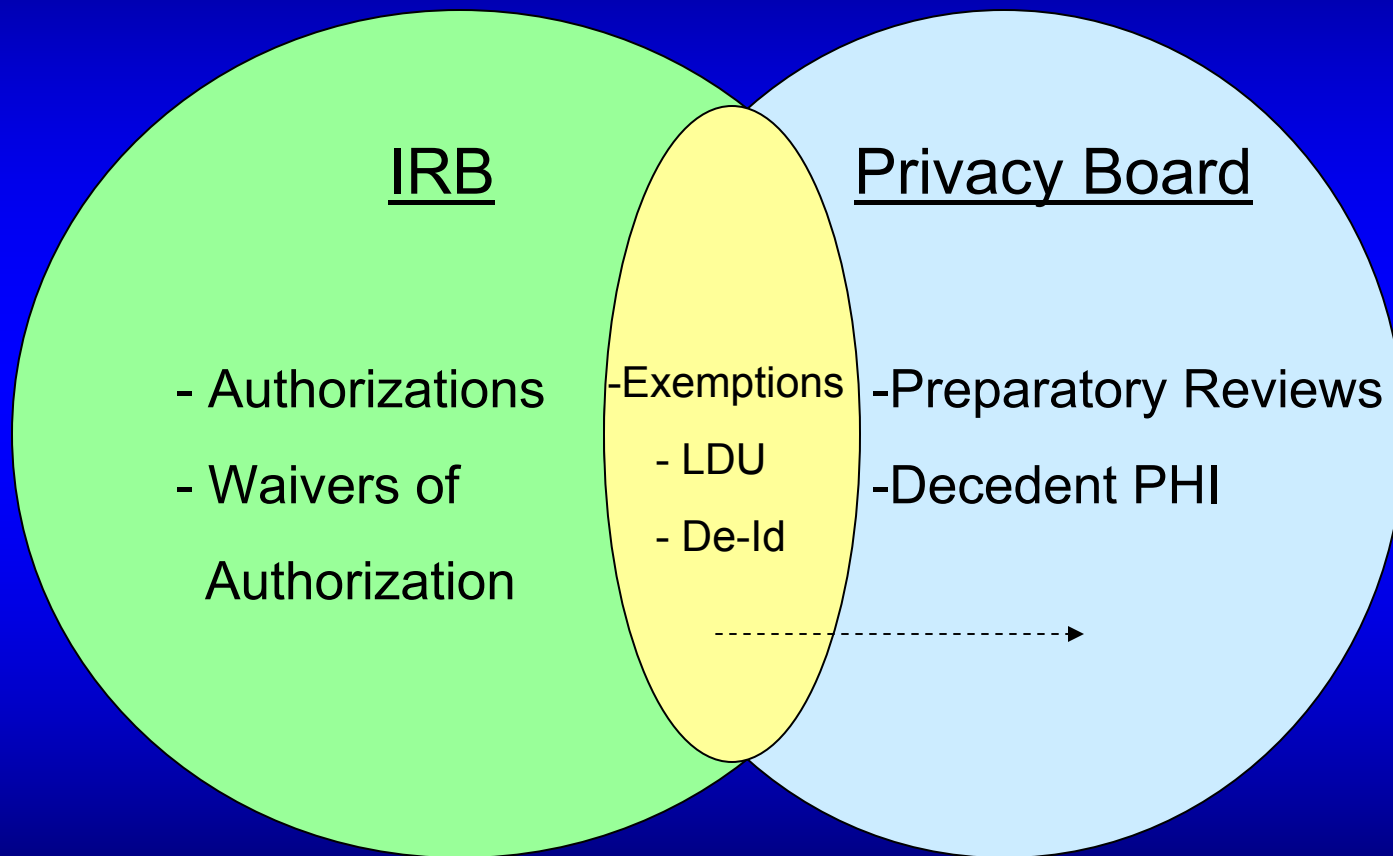
Upstate Medical University HIPAA Implementation

- Almost all components within the SUNY Health Care Component HIPAA hybrid entity.
- Research function is within the HCC
 - HIPAA PHI transfer to researchers apply
 - All HIPAA protections of PHI apply
- Oversight of PHI access mechanisms split
 - IRB
 - Privacy Board
 - Privacy Officer



Upstate Medical University

Research access to PHI



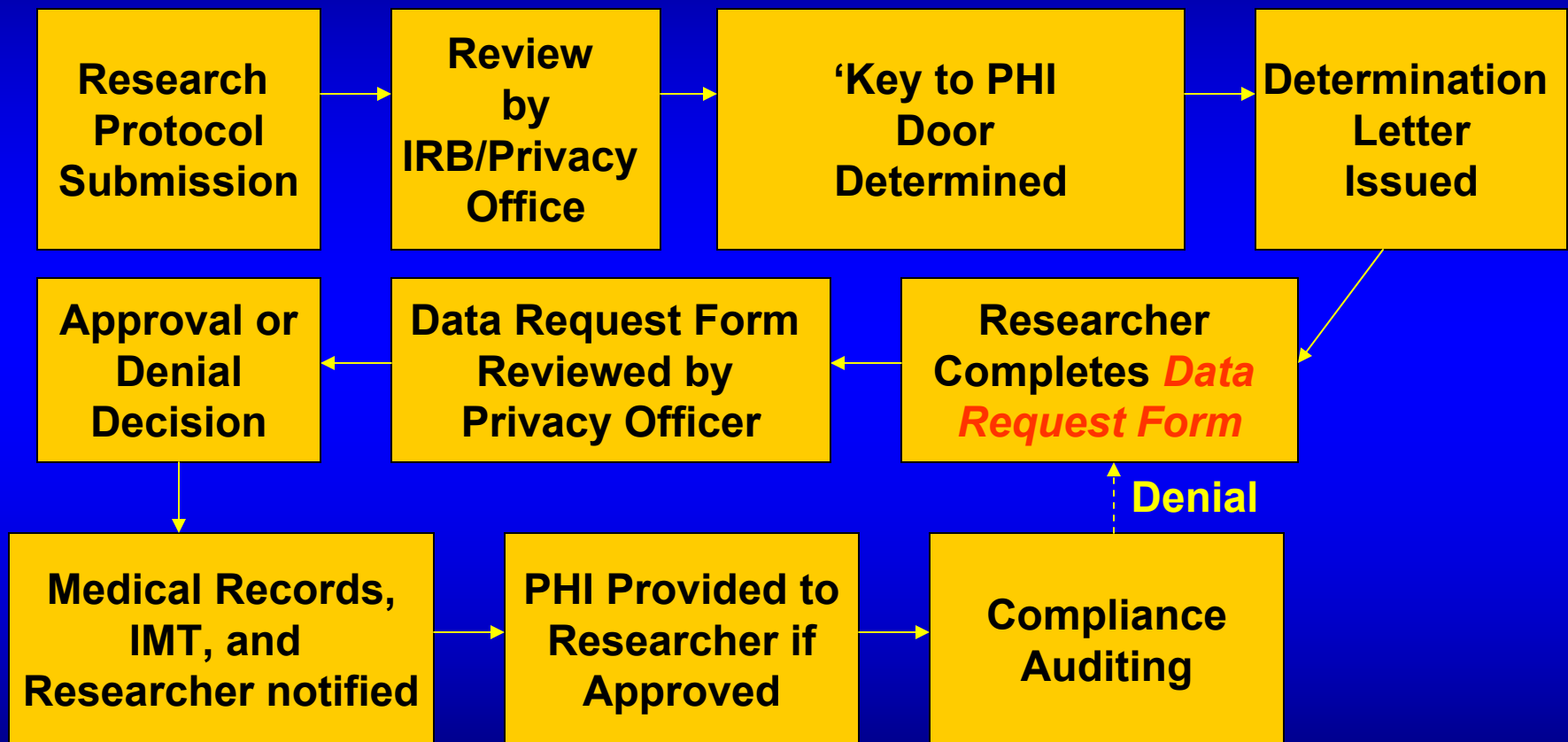
Human Subject Research

Privacy Oversight & Compliance



December 5, 2003
Washington DC

Upstate Medical Center Research access to PHI



University at Buffalo

HIPAA Implementation (1)

- Almost no components within the SUNY Health Care Component HIPAA hybrid entity.
- Research function is outside of the HCC
 - HIPAA PHI transfer to researchers apply
 - Only HIPAA PHI transfer protections apply
- Oversight of PHI access mechanisms consolidated in IRB (subject to review by Director of HIPAA Compliance).



UB – Research not in Covered Function?!

- SUNY/UB employs faculty, not health care providers.
 - Exceptions: Dental Medicine and Student Health services.
- Independent corporate entities employ health care providers, not faculty.
 - 21 independent medical/dental practice plans.
 - Partnered teaching hospitals (>9).
- UB cannot ‘claim’ a separate entity’s health care provider when defining the SUNY covered function.
 - UB research is outside of a HIPAA covered function.
 - SDM research given same legal treatment to remain consistent, but voluntarily adheres to HIPAA.



University at Buffalo

HIPAA Implementation (2)

- UB Research and provision of Health Care *defined* as separate functions.
- UB Research is *defined* as not being part of the HIPAA Health Care Component within the SUNY hybrid entity.
- UB Health Care covered function:
 - School of Dental Medicine clinical & educational activities.



University at Buffalo

HIPAA Implementation (3)

- The research function and the health care function may both be present in a particular research protocol
 - Requires PHI to flow from health care to research using one of 7 “keys” which permit this transmission.
- UB IRB responsible for ensuring proper use of 7 “keys”.
- UB IRB serves several affiliated hospitals:
 - Hospitals rely on UB IRB to ensure access “keys” are in place for each protocol.
 - Other Hospitals have separate IRB/HIPAA structures which UB researchers must navigate.



University at Buffalo

Research Access to PHI

IRB

- Authorizations
- Exemptions
- Waivers of Authorization
- LDS/DUA
- Preparatory Reviews
- De-Ident
- Transition provisions
- Decedent PHI

Human Subject Research & Privacy Oversight & Compliance



December 5, 2003
Washington DC

SUNY UB

Access To PHI For Research



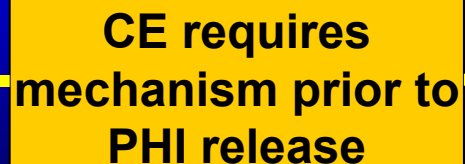
UB IRB Denial



UB IRB approval

3rd party IRB approval of traditional research component (if applicable)

UB CF or external CE Firewall



December 5, 2003
Washington DC

Duke University

HIPAA Implementation

- Duke University – hybrid covered entity
 - Duke Health Enterprise is the covered function, which includes the health system, School of Medicine, and affiliated organizations
 - Non-health care University activities are outside of the covered function
- IRB is given responsibility relative to HIPAA implementation in research



Common Rule vs. Privacy Rule

<u>COMMON RULE</u>	<u>PRIVACY RULE</u>
Applies to federally supported or FDA regulated research. In institutions/sites with an MPA or FWA, applies to all research.	Applies to all research within Covered Entities.
Protects interests and welfare.	Protects privacy rights and welfare.
Human subject: A living individual about whom an investigator obtains data.	Individual: subject of protected health information; a living or deceased person.
Institutional Review Boards (IRBs).	Uses IRBs <u>or</u> Privacy Boards.
Continuing review at least annually.	No requirement for continuing review.
Informed Consent.	Authorization.
Data recording exempt if done so “in manner that subjects cannot be identified”.	Data recording exempt if de-identified.



How may the IRB guide an Investigator to reduce the impact of the Common Rule and the Privacy Rule (HIPAA) on her/his research?



Common Rule / Privacy Rule Considerations

An Activity Does Not Prompt Either
Common Rule or Privacy Rule
(HIPAA) Considerations Requiring
IRB Review When:

- **The activity is not research; OR**
- **The research does not involve a human subject AND**
- **The research does not involve PHI.**



Definition of "Research"

45 CFR 46.102 (d) and 164.501

A systematic investigation ... designed to develop or contribute to generalizable knowledge.



Common Rule / Privacy Rule Considerations (2)

An Activity Does Not Prompt Either Common Rule or Privacy Rule (HIPAA) Considerations Requiring IRB Review When:

- The activity is not research; OR
- **The research does not involve a human subject AND**
- **The research does not involve PHI.**



Consider how an investigator may reduce the impact of the Common Rule and the Privacy Rule (HIPAA) by focusing on research involving use of a database or a sample repository.



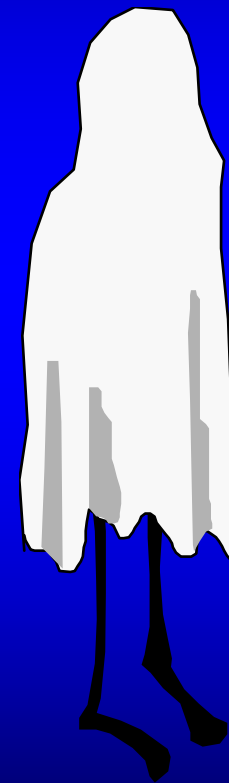
Real Administrative Simplification

Ensure that Information Associated with the Data/Samples is Modified so it Does Not Relate to a “Human Subject” and Either Does Not Involve PHI or is Presented as a Limited Data/Sample Set.



Regarding the Common Rule

- Anonymize (unlink) the data/samples.
- Establish conditions whereby subject identity cannot readily be ascertained.



Anonymize (Unlink) the Data/Samples

- Remove all identifiers or codes that directly or indirectly link a particular data point or sample to an identifiable person.
- These data/samples become irreversibly unlinked from any subject identifiers.



Establish Conditions So Subject Identity Cannot Readily Be Ascertained

Provide two declarations to the IRB:

- From the keeper of the data/samples declaring that the recipient has not been given and will not be given a link to permit subject identification.
- From the recipient of the data/samples that he/she does not have and will not seek access to the identity of subjects.
- <http://ohrp.osophs.dhhs.gov/humansubjects/guidance/stemcell.pdf>



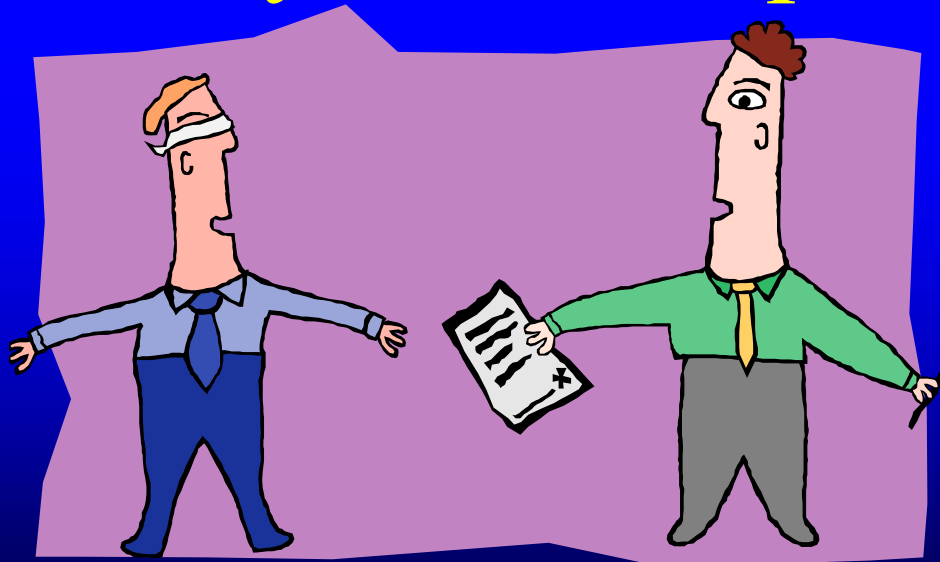
Regarding the Privacy Rule

- Modify Data/Samples so they do not involve PHI.
- Establish a Limited Data/Sample Set and a Data Use Agreement.



Modify Data/Samples So They Do Not Involve PHI

- Remove health information.
- De-identify data/samples.



Establish a Limited Data/Sample Set and a Data/Sample Use Agreement

- Remove direct personal identifiers.
- Remove postal address information other than town or city, State and zip code.
- Note: All elements of dates, any age, and an identifying code related to the person are permitted.

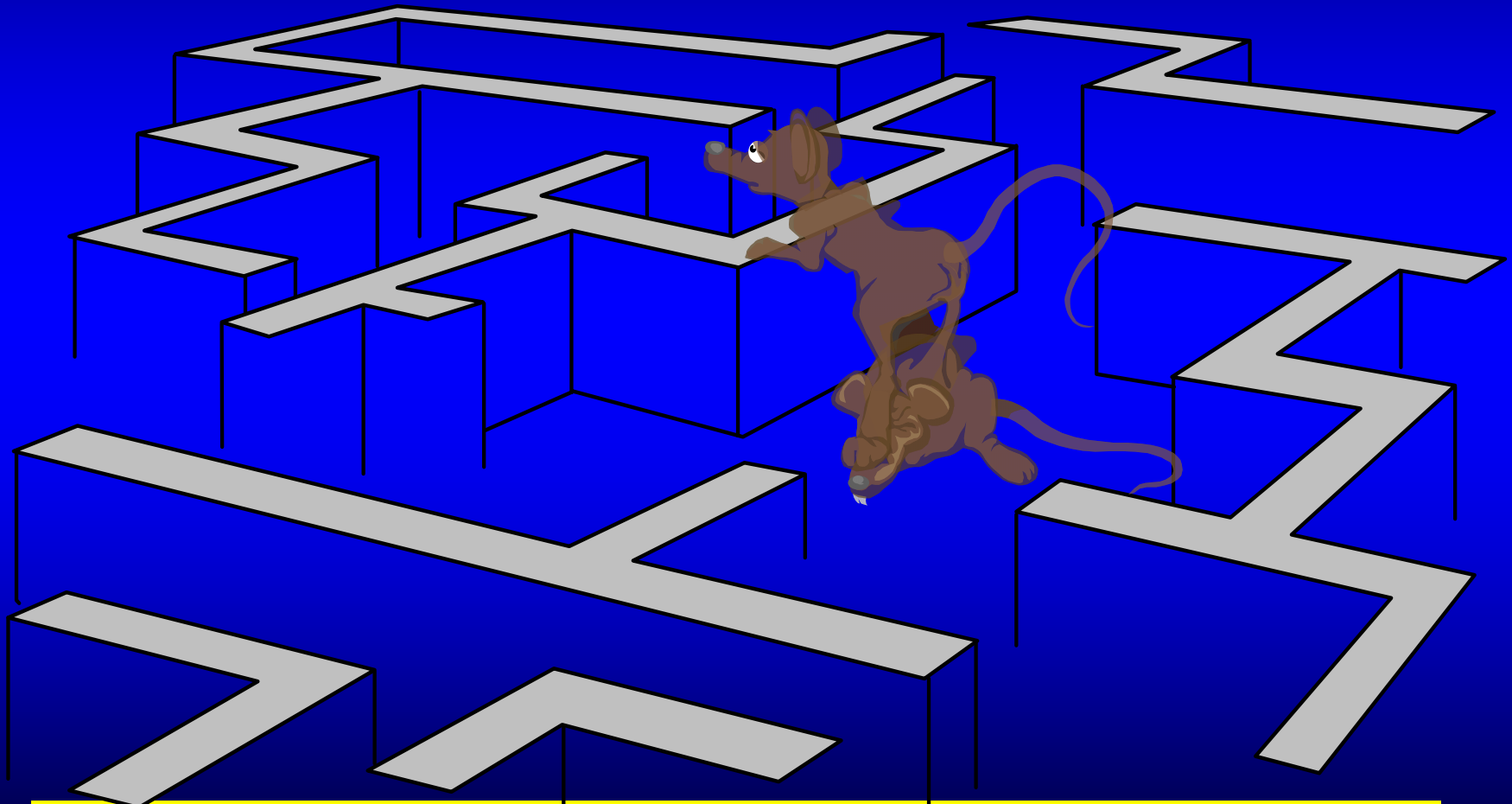


Satisfy Common Rule & Privacy Rule

- Establish conditions so subject identity cannot readily be ascertained.
- Establish a limited data/sample set and a data/sample use agreement.



Questions?



December 5, 2003
Washington DC

Contact Information

- John Falletta, MD
 - falle001@mc.duke.edu
 - <http://irb.mc.duke.edu>
- Tammy Sayers Lesko
 - tlesko@copernicugroup.com
 - <http://www.copernicugroup.com>
- Brian Murphy, MS
 - bwmurphy@buffalo.edu
 - http://www.hpitp.buffalo.edu/hipaa/UB_HIPAA_ResearchHomePage.htm

