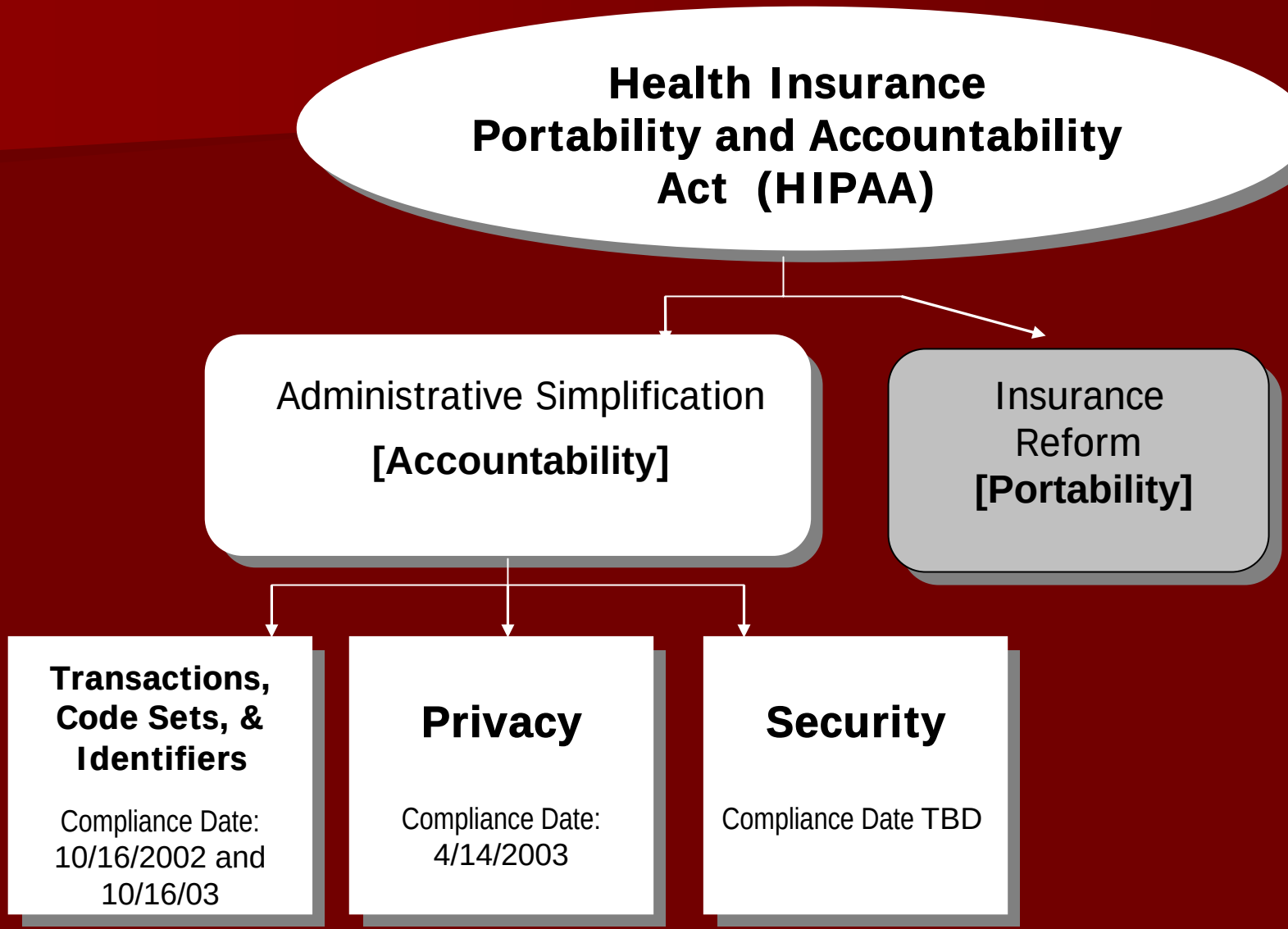
National Institute on Aging

Research under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”)

HIPAA Overview



PRIVACY vs. SECURITY

- **PRIVACY**

  Refers to ***WHAT*** is protected — Health information about an individual and the determination of WHO is permitted to use, disclose, or access the information

- **SECURITY**

  Refers to ***HOW*** private information is safeguarded—Insuring privacy by controlling access to information and protecting it from inappropriate disclosure and accidental or intentional destruction or loss.

PRIVACY

- Due to the constraints imposed by scope of HIPAA, privacy regulation is applicable only to:
  - **"Covered" Entities** — Healthcare Providers, Health Plans, and Clearinghouses
  - **"Protected" Health Information (PHI)** — Transmitted or maintained in any form or medium (includes paper and oral)
  - **"Floor" of Provisions** — Does not preempt more stringent state laws, potentially requiring some dual systems

PRIVACY

WHO is Covered?

- **"Covered Entities"** = A Health Plan, Healthcare Clearinghouse, or a Health Care Provider who transmits any health information in electronic form in connection with a transaction covered under HIPAA

- Covered entities are required to contractually bind other entities with whom they share PHI format ("Business Associates Contracts")

PRIVACY

WHAT does the Privacy Rule COVER?

- **Protected Health Information (PHI)** = Individual (Patient) identifiable information relating to the past, present or future health condition of the individual

- ALL information whether maintained in electronic, paper or oral format

PRIVACY

WHAT does the Privacy Rule MEAN?

- Limits the **Use** and **Disclosure** of PHI
- Establishes Individual's (Patient) right to control access and use of PHI
  - Right to inspect or copy PHI
  - Right to amend incorrect information
  - Right to receive an accounting of all disclosures made for reasons other than payment, treatment, or health care operations

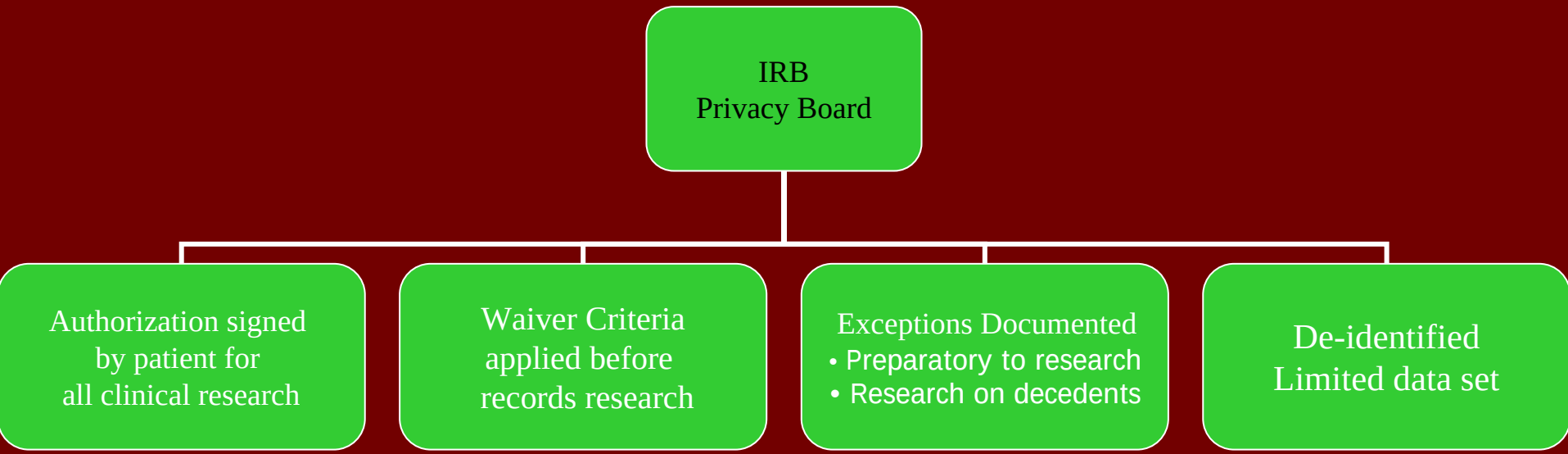
PRIVACY

WHAT does the Privacy Rule MEAN? (cont'd)

- Balances health information protection and individual rights against public health and safety needs

- Administrative Requirements
  - Privacy Officer
  - Notice
  - Training & Sanctions
  - Safeguards
  - Policies & Procedures

HIPAA and Research



HIPAA Authorization

Authorization signed by patient for all clinical research

- Patient authorization elements
  - The information
  - Who may use or disclose the information
  - Who may receive the information
  - Purpose of the use or disclosure
  - Expiration date or event
  - Individual's signature and date
  - Right to revoke authorization
  - Right to refuse to sign authorization
  - Redisclosure statement

HIPAA Authorization

- The information
  - Relates to “minimum necessary standard” (we will use only the PHI we need to for the research)
- Who may use or disclose the information
  - “the PI and the research team”
- Who may receive the information
  - The sponsor/CRO/central labs/etc.

HIPAA Authorization

- Purpose of the use of disclosure
  - Short description of research
- Expiration date or event
  - “end of study”; “never” for databases
- Individual’s signature and date
  - Subject must receive signed copy
  - Must be retained for 6 years

HIPAA Authorization

- Right to revoke authorization
  - Must be made in writing
  - Reliance exception
- Right to refuse to sign authorization
  - If refusal exercised, research related treatment can be withheld
- Redisclosures not protected
  - Statement that redisclosures may happen and their PHI would no longer be protected

HIPAA Waiver of Authorization

Waiver Criteria applied before records research

- Most likely to be used in cases of research involving retrospective chart reviews
- IRB/Privacy Board may also waive authorization to allow use of PHI by third parties to recruit study subjects—no waiver or authorization needed to recruit your own patients into a clinical trial

HIPAA Waiver Criteria

Waiver requires IRB/Privacy Board approval and documentation of three (3) waiver criteria:

1. Use or disclosure involves no more than minimal risk to privacy of the subject based on, at least:
   a) Adequate plan to protect the information from improper use and disclosure;
   b) Adequate plan to destroy identifiers; and
   c) Written assurances that the PHI will not be disclosed further than as set forth in the waiver

HIPAA Waiver Criteria, con't

2. The research could not practicably be conducted without waiver or alteration

3. The research could not practicably be conducted without access to and use of the PHI

Note: HHS intends to issue future guidance for IRBs and Privacy Boards on applying waiver criteria

Authorization and Waiver exceptions

Exceptions Documented
- Preparatory to research
- Research on decedents

- There can be no disclosure of PHI to researchers from CU or NYPH without authorization or waiver unless the disclosure is for:
  1. Preparatory research—i.e., to assess feasibility of research or formulate a research hypothesis; or
  2. Research on a decendent

Reviews Preparatory to Research

- CE obtains a representation from the researcher that:
  - Use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol;
  - No protected health information is to be removed from the covered entity by the researcher in the course of the review; and
  - The protected health information is necessary for the research purposes.

Research with Decedent's Information

- CE obtains from the researcher:
  - Representation that the use or disclosure is sought is solely for research on decedents;
  - Documentation of the death of such individuals; and
  - Representation that the protected health information for which use or disclosure is sought is necessary for the research purposes.

De-Identified Health Information

De-identified
Limited data set

1. If information is “de-identified” in accordance with “generally accepted statistical and scientific principles or methods” (see HHS guidance: Report on Statistical Disclosure Limitation Methodology available at www.fcsm.gov/working -papers/wp22.html)

2. If all identifiers listed in a “safe harbor” are removed—this safe harbor requires the removal of 18 identifiers (of limited use)

3. Dummy identifier to facilitate linkage within CE permitted

Limited Data Set

- Permits identifiers not permitted by de-identification safe harbor such as:
  - Zip code, town, city & state, date of birth/death and dates of service
- Benefit: no need for waiver or authorization if only disclosing a limited data set to a researcher; accounting rule doesn't apply
- Requires a "data use agreement" with the intended recipient

Limited Data Set

- Data Use Agreement
  - limiting the use of disclosed data consistent with the purposes of research (minimum necessary standard applies)
  - Limits who can use or receive the data
  - Requires the recipient to agree not to re-identify the data or contact the individuals
  - Must contain adequate assurances similar to BA requirements that intended recipient will use adequate safeguards to prevent unauthorized use or discloser of data

Limited Data Set

- Authorized for public health, research, and health care operations purposes:

1. Public health uses—disease registries maintained by private sector or universities or other types of studies for public health purposes

2. Possible health care operations use—hospital sharing of limited data set information with local hospital association

3. Possible research use—establishment of research databases and repositories

Other Considerations

- Accounting rule
- Minimum Necessary standard

Accounting Issue

- *Use*
  - Within Columbia University healthcare component
  - Not tracked for accounting to the individual
- *Disclosure*
  - Outside Columbia University healthcare component
  - Research is not considered in the healthcare component

Accounting of Disclosures

- "An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested, except ..."

- TPO disclosures, authorization disclosures, limited data set disclosures, disclosures required by law & disclosures requested by the individual excepted from accounting (see 164.528 for additional items)

Accounting Issue

- Conclusion on accounting rule—applies to research waivers as well as preparatory and decedent exceptions; permits streamlined response where:
  - At least 50 records involved in waivers

- Streamlined response must include:
  - Name of study or protocol
  - Purpose of Study
  - Type of PHI sought
  - Timeframe

Minimum Necessary Standard

- Minimum Necessary Standard = Need to know basis
- Minimum Necessary Standard does not apply to uses and disclosures for treatment or pursuant to authorization
- Like the accounting rule--applies to research waivers as well as preparatory and decedent exceptions

Columbia University Health Sciences

Hybrid Entity

- *Hybrid entity* means a single legal entity that is a covered entity and whose covered functions are not its primary functions.
- First step in a Academic Medical Center location is to define your covered entity.
- For CU, the hybrid structure was the right fit.

Hybrid Entity

- Who is in and who is out and what are the ramifications of being out?
- At CU, we choose to exclude research from the healthcare component of our covered entity
- Rationale:
  - disclosures to researchers of clinical data must go through rules previously discussed regardless of whether research is in or out of covered functions
  - HIPAA has criminal penalties

Organized Health Care Arrangement (OHCA)

- Strategy: Joint OHCA comprised of—
  - Columbia University Health Sciences
  - Cornell University Medical School
  - NYPH (Cornell Medical Center & Columbia Presbyterian Medical Center)
- Defines boundaries for TPO, research, marketing and fundraising
- PHI sharing for healthcare operations within OHCA expanded somewhat
- Permits shared Notice of Privacy Practices

HIPAA and Research

- PHI sharing for research is a disclosure regardless of whether inside the OHCA or to investigators or other entities
- Disclosures for research can only occur after documentation that authorization, waiver or exception has been met
- Mechanisms must be in place by 4/14/03

Parameters Governing Proposed Strategy

- Clinical investigation continues without undue burden/cost to investigators at CPMC
- NYPH is satisfied that high security and low cost to NYPH are addressed
- Data flows are auditable to document compliance

Issues raised for Columbia University

- Who will be applying these new standards?
- How will these new standards and procedures be communicated to the research community?
- How will the disclosing entity know that a researcher has been approved *before* disclosing PHI?
- What sanctions will exist to discourage violations?

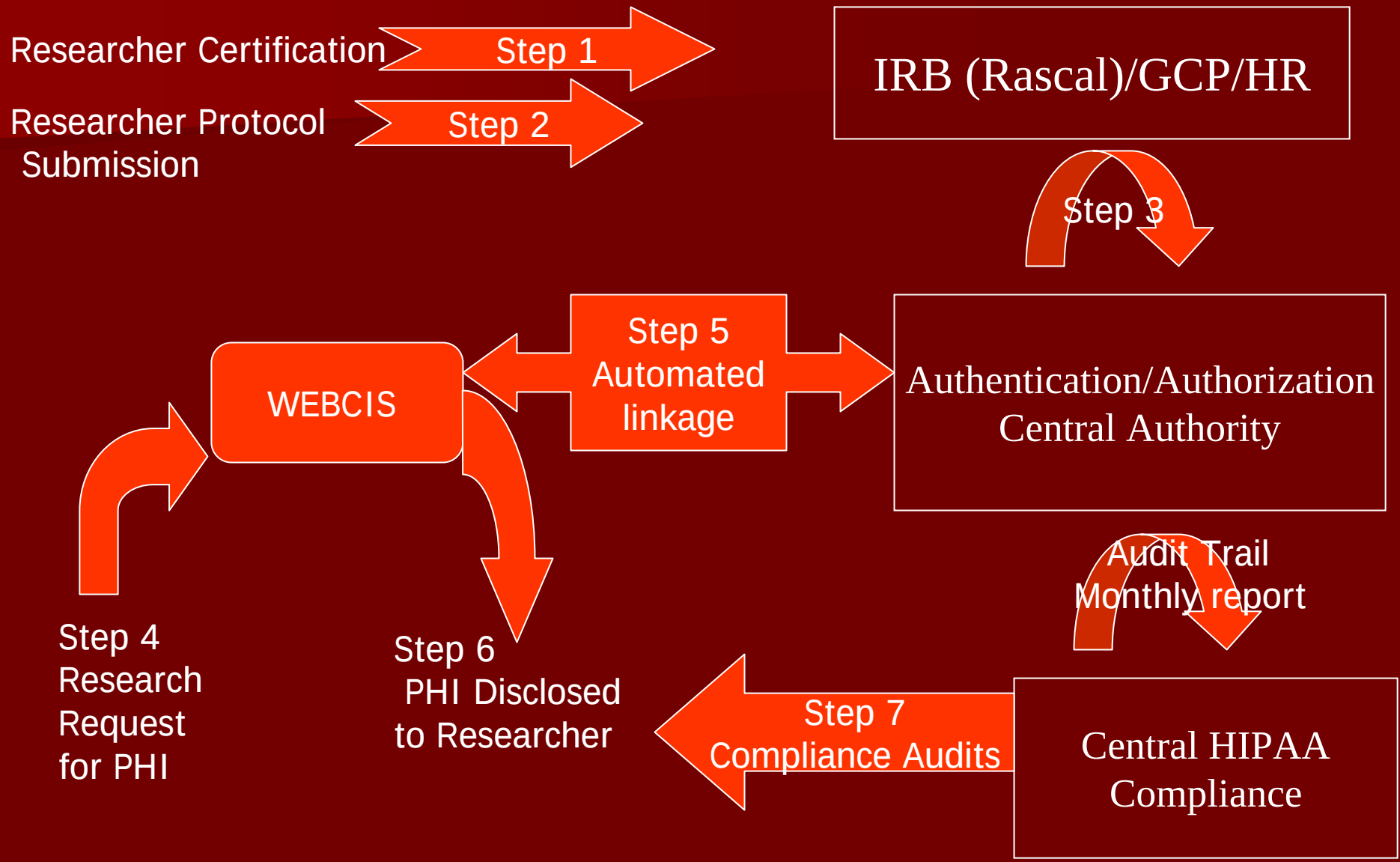
Role of the IRB

- No privacy board
- IRB to approve HIPAA authorization for clinical research disclosure as part of consent form
- IRB to approve HIPAA waivers for medical records research and recruitment activities
- All research involving human subjects must be reviewed and approved by the IRB

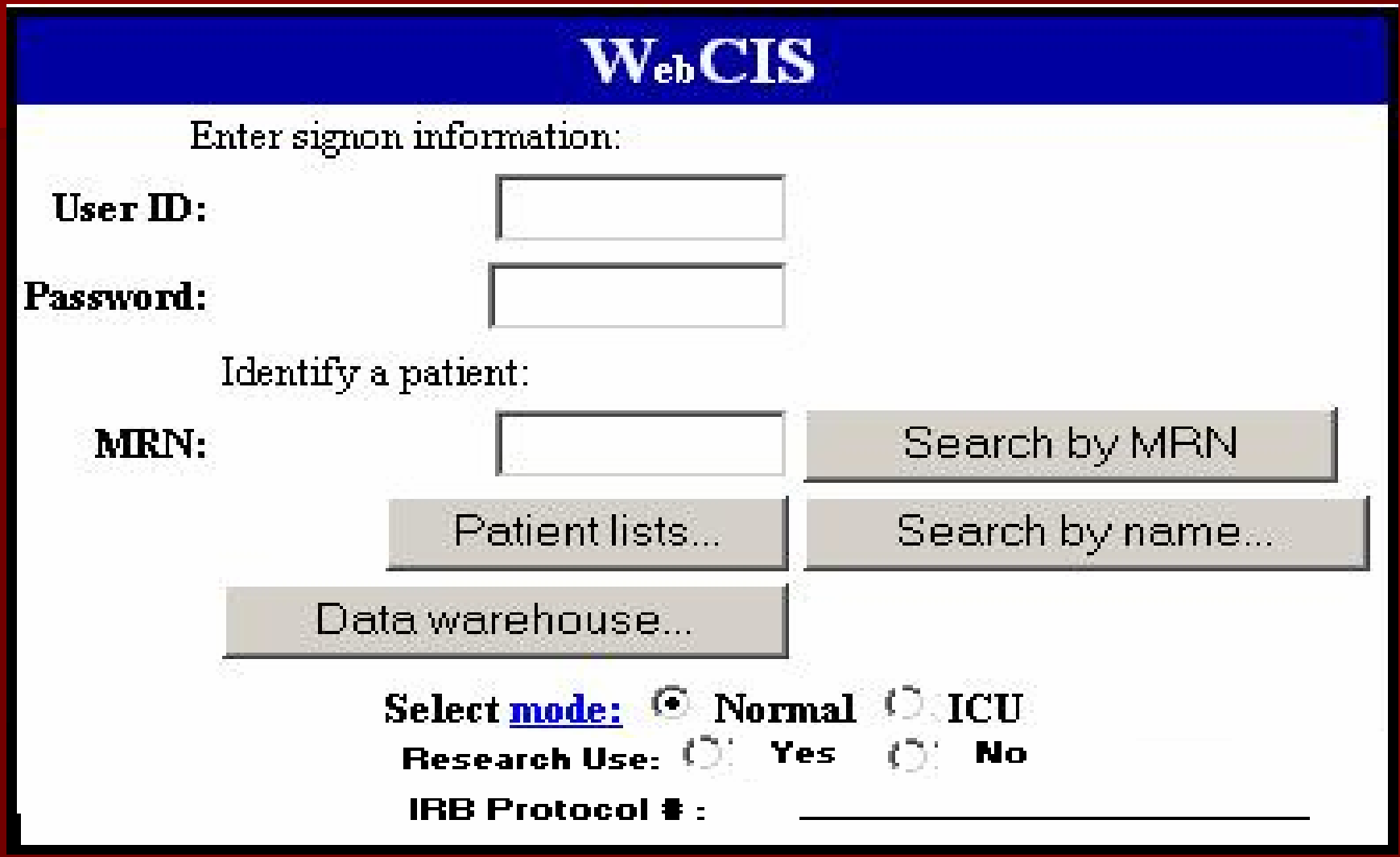
Disclosure of PHI for Research

- View of Individual PHI
  - TPO
  - Authorization
- Batch transfer of PHI
  - TPO
  - Authorization
  - Waiver
  - Preparatory/Decedent

Research Data Flow—Individual Query



View of Individual PHI



Research Access to WebCIS Denied

- IRB protocol not valid
- User GCP* certification not valid
- User not authorized to access patient data under IRB protocol
- User not a current CU or NYPH employee

* Good Clinical Practice course includes a HIPAA research training module

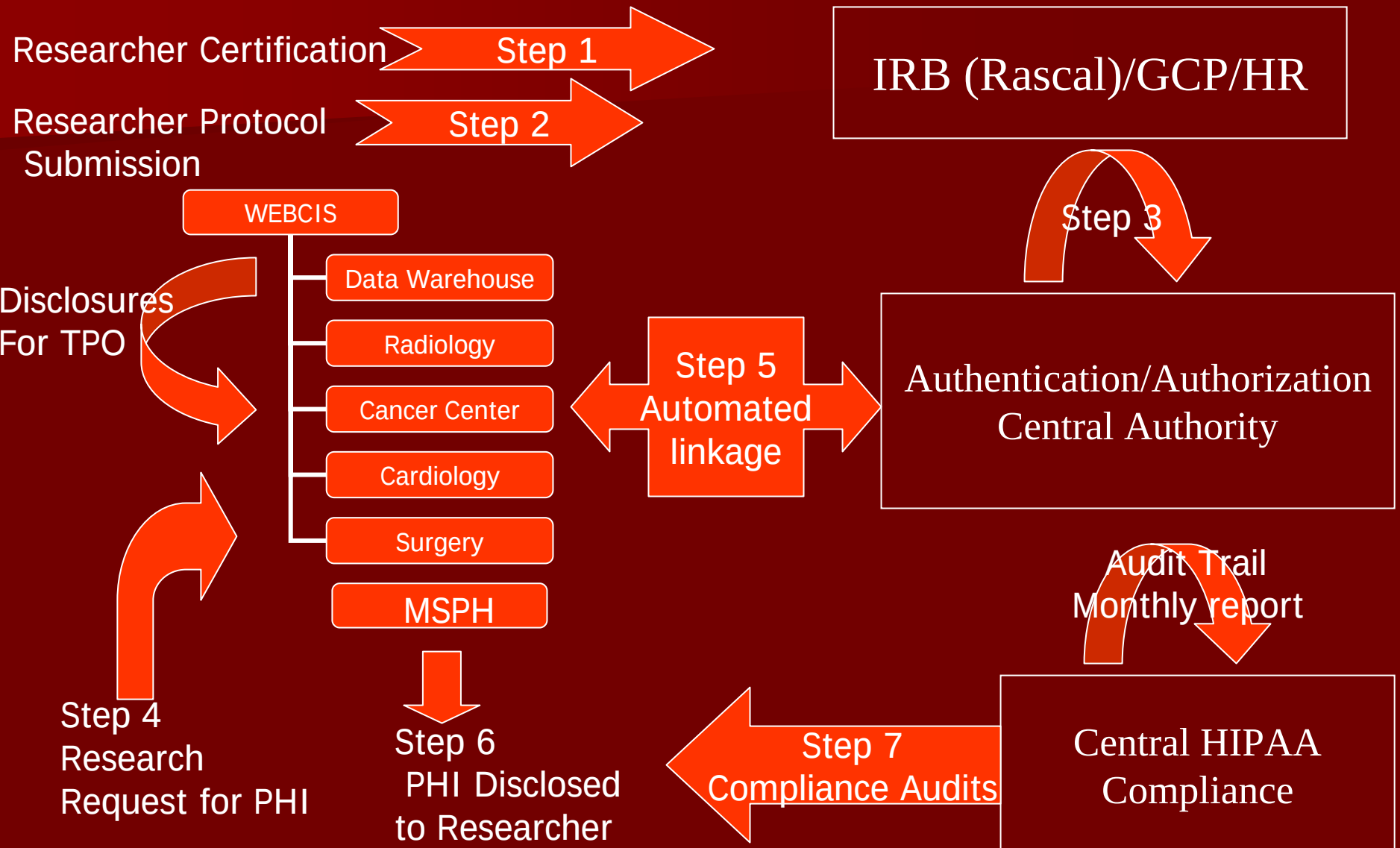
Batch Transfers of PHI for Research

- WebCIS provides data feeds to the Warehouse and other intermediary servers (e.g., Cancer Center, cardiology, Surgery, Radiology)
- These servers support TPO and research using the same or overlapping data
- Issues:
  - Security and certification of the servers
  - Transfer of data from WebCIS to servers

Batch Transfers of PHI for Research

- Issues, cont'd
  - Use of data on servers for research
  - Downloading of data from servers to other servers or PCs (disclosures)

Research Data Flow—Batch Query



Security Certification of the Servers

- Certification standards and authority: S. Sengupta and J. Davis
- Certification/re-certification annually
- Physical security
- Training and certification of data managers
- Authorization/Authentication from central Authentication authority (not local)

Security Certification of the Servers

- Interface with IRB (Rascal*), GCP, and HR to verify IRB protocol, GCP training, and current employment
- Audit trail of all disclosures in standard format output to central audit authority

* Rascal is a CU proprietary research administration database which electronically administers the research at CU (e.g., training, COI forms, proposal approval, etc...)

Implications for CU

- No paper
- Minimal burden on investigators
- Acceptable to NYPH
- HIPAA compliant
- New interfaces required
- Intermediate servers will require some programming and potentially security upgrades

Questions & Answers

Jeffrey P. Davis, Esq.
Associate Vice President/Privacy Officer
Columbia University Health Sciences
212-305-7315
jd2086@columbia.edu