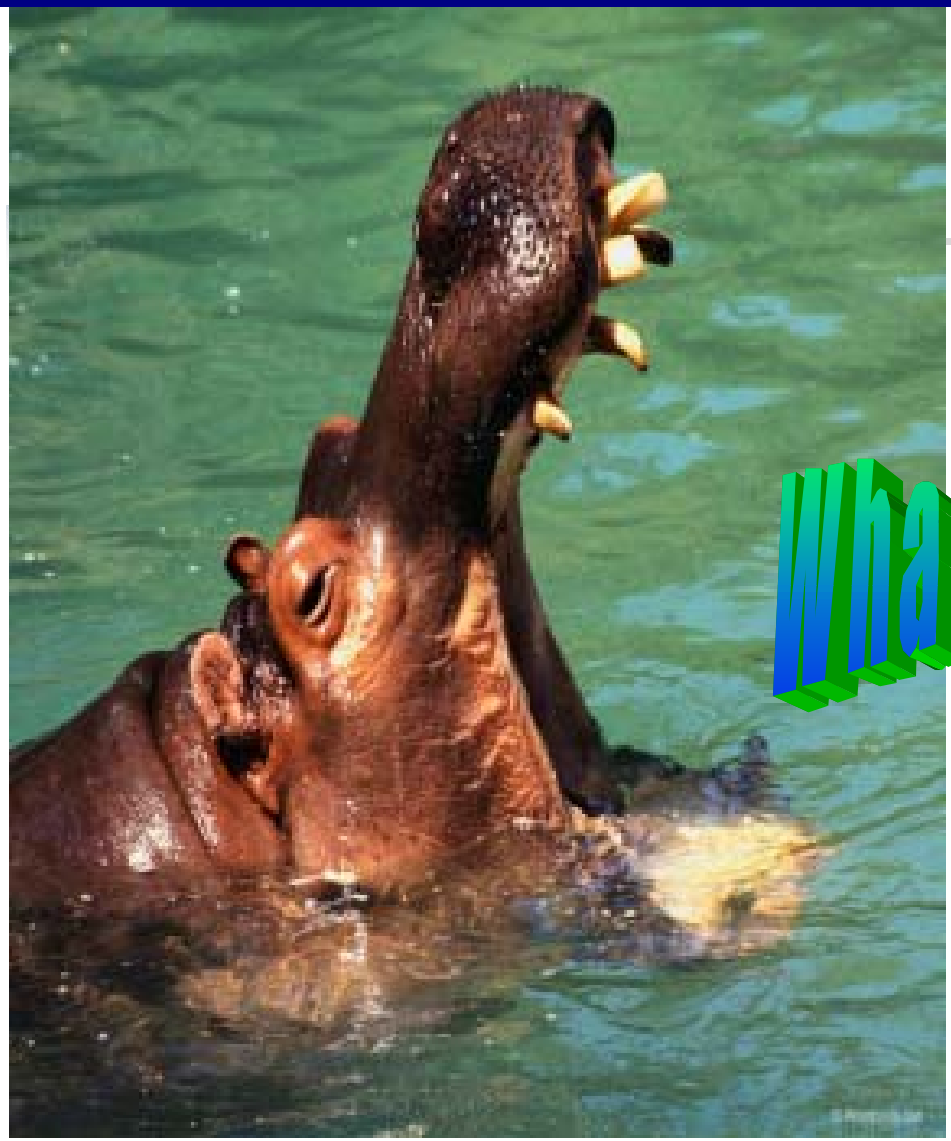
Implications of the Health Insurance Portability and Accountability Act of 1996

Mark Weiner, M.D.
Assistant Professor of Medicine
University of Pennsylvania
mweiner@mail.med.upenn.edu

Computer Science 495
Special Topics in CS: Medical Informatics
February 21, 2002



What's a HIPAA?

What is HIPAA

- Health Insurance Portability and Accountability Act of 1996
- proposed by Sen. Edward Kennedy (D-MA) and Nancy Kasselbaum (R-KS)
  - Focused on issues involving
    - obtaining new insurance at new job with pre-existing conditions
    - protection from fraud
    - administrative simplification
      - Electronic transmittal of data for billing purposes
      - Privacy issues related to transmission of clinical data

What Information is covered under HIPAA

- Personal Health Information (PHI)
  - Anything that can potentially identify an individual

Name

Zip code of more than 3 digits

Dates (except year)

Telephone and fax numbers

Email addresses

Social Security Numbers

Medical Record Numbers

Health Plan Numbers

License numbers

Privacy vs. Security

- Privacy
  - Administrative mechanisms that govern the appropriate use and access to data
    - Not all hospital employees need to know everything about a patient
- Security
  - Technical mechanisms to ensure privacy
    - don’t have a fax machine that receives personal information in a public place
    - Encrypt electronic communications

Privacy before HIPAA

4th Amendment (…secure in their persons, houses, papers and effects against unreasonable searches and seizures…)
Fair Credit Reporting Act (1970)
Privacy Act (1974)
Family Educational Rights and Privacy Act (1974)
Right to Financial Privacy Act (1978)
Privacy Protection Act (1980)
Electronic Communications Privacy Act (1986)
Video Privacy Protection Act (1988)
Employee Polygraph Protection Act (1988)
Telephone Consumer Protection Act (1991)
Driver's Privacy Protection Act (1994)
Telecommunications Act (1996)
Children's Online Privacy Protection Act (1998)
Identity Theft and Assumption Deterrence Act (1998)
Gramm-Leach-Bliley Act (1999)

Gaps in privacy protection

- Most of the preceding laws protect aspects of personal information (mostly financial), but not Health Information
- Inconsistent State laws exist for protection of information regarding certain health conditions -- HIV, Mental Illness, Cancer

Concern about loss of Privacy

- 1998 National Survey
  - 33% concerned about the amount of information being requested from various sources
  - 55% VERY concerned
- 1995 Survey
  - 80% agreed with statement that they had lost all control of their medical information

Concern About Loss of Privacy

- 1999 Survey
  - What issues concerned them the most in the coming century?
    - 29% listed “Loss of Personal Privacy” as 1st or 2nd concern
    - 23% or less selected terrorism, world war, global warming

Concern About Loss of Privacy

- Internet usage (1999 survey)
  - 82% have used a computer
  - 64% have used the internet
  - 58% have sent e-mail
  - 59% worry that an unauthorized person will gain access to their information
  - 75% of people visiting health sites are concerned that information is being shared

Concern About Loss of Privacy

- Electronic Medical Records/Data Banks
  - 75% express concern about insurance companies putting information about them in a database accessible by others
  - 35% of Fortune 500 companies look at medical records before making hiring or promotional decisions

Concern About Loss of Privacy

- Genetic information
  - 85% concerned that insurers and employers may gain access to personal genetic information
  - 63% would not take genetic screening tests if the information was going to be shared with insurers and employers
  - 32% of eligible people refused to have genetic testing for breast cancer risk because of privacy concerns

Are These Privacy Concerns Unfounded?

- 1999- A Michigan based Health System accidentally posted medical records of thousands of patients on the Internet
- A Utah-based pharmacy benefits management company used patient data to solicit business for its parent company -- a drug store

Are These Privacy Concerns Unfounded?

- Health Insurance Claims forms blew out of a truck on its way to a recycling center
- A patient in a Boston-area hospital discovered that her medical record had been read by more than 200 hospital employees
- A Nevada woman purchased a used computer that still had prescription records from the pharmacy that formerly owned the computer

Are These Privacy Concerns Unfounded?

- Johnson and Johnson markets a list of 5 million names and addresses of elderly incontinent women
- A few weeks after undergoing a blood test, an Orlando woman received a letter from a drug company promoting their treatment for high cholesterol

Are These Privacy Concerns Unfounded?

- A banker who also sat on a county health board identified people with cancer and called in their mortgages!
- A physician diagnosed with AIDS had his surgical privileges suspended (Medical Center of Princeton)
- A newspaper published the history of psychiatric treatment and suicide attempt of congressional candidate

Why does electronic communication increase privacy concerns?

- Problems with paper charts - Messy, difficult to find, one physical copy - all make it harder to acquire and disseminate information
- Electronic documents can be intentionally or unintentionally transmitted to thousands of people at once

What is HIPAA designed to do?

- Give patients more control over use of data
- Set boundaries on uses and disclosures of data
- Establish safeguards to protect data
- Establish accountability for privacy breaches
- Balance privacy with social responsibility

HIPAA Timeline

- 1996 - HIPAA Signed into law
  - Privacy regulations not specified
  - Congress was to enact laws and policy regarding privacy by 1999
  - If Congress failed to develop standards, task would fall to Department of Health and Human Services (DHHS)
- 1999 - DHHS becomes responsible for developing privacy regulations

HIPAA Timeline

- 1999 - DHHS proposes privacy standards and opens them up for public comment
- 1999-2000 DHHS receives 50,000 comments on regulations
- December 2000 - DHHS publishes “Final Privacy Rule”
- February 2001 - Enactment of Final Rule delayed because of “administrative difficulties.” Further public comment requested

HIPAA Timeline

- April 2001 - Privacy Rule implementation phase begins
- April 2003 - Deadline for covered entities to complete implementation plan

HIPAA Stipulations for Using and Releasing Information

- Notification
- Consent
- Authorization

HIPAA Stipulations for Using and Releasing Information

- Notification
  - Informing patients in simple language regarding the manner in which their data is handled

HIPAA Stipulations for Using and Releasing Information

- Consent
  - one time, general agreement to use the patient's information in treatment. For payment, or for "healthcare operations"
  - Lasts indefinitely, necessary for treatment
  - Sharing information between primary care physician and consulting specialist
  - Regulations allows provision of care to be conditioned on patient's consent to use information for payment purposes.

HIPAA Stipulations for Using and Releasing Information

- Authorization
  - limited in time and scope
  - Non-routine purpose
  - Example : Patient is actively participating in a research protocol and personal health information will be shared with a clinical service or university

Health-related activities covered by HIPAA

- Health Care
- Billing
- Marketing
- Fund Raising
- Research

HIPAA In Health Care

- Consent to release information to insurance carriers for billing purposes
- Primary and consulting physicians given full access to record for treatment purposes
- Hospital Staff provided “minimum necessary” information to conduct business
- Laboratories and Radiology offices can use information for billing purposes
- Stipulations about auditing of who has seen/used what information

HIPAA In Health Care

- Fax machines
- Hospital information networks
- E-mail
- Physical security of computer hardware

Research under HIPAA

- Continues as before when appropriate informed consent is obtained from subjects.
- Special consideration necessary when using data without explicit consent of subjects
  - Few restrictions when using de-identified data on populations of patients (no names, SSNs, addresses; birthdates; populations must have substantial size)
  - Oversight required to use identifiable data

Research under HIPAA

- Patient consent NOT required with identifiable data when all of the following are true:
  - IRB approves protocol and use of data
  - use or disclosure of data presents minimal risk
  - will not affect privacy and welfare of individual
  - consent process impractical
  - research could not be conducted without information
  - plan exists to protect identifiers from improper use and disclosure
  - Data will not be reused for other purposes without authorization from IRB

HIPAA in Research Summary

- Little oversight needed for de-identified, population-based data
- IRB authorization required to access identifiable patient information
- Duty to inform patients regarding research uses of their data
- Audit trails of information access for research
- ??? Responsibilities when initiating patient contact based on knowledge of personal information

Accountability

- Civil penalties
  - Violation of standards will be subject penalties of $100 per violation, up to $25,000 per person, per year for each requirement or prohibition violated.

Accountability

- Federal criminal
  - up to $50,000 and one year in prison for obtaining or disclosing protected health information
  - up to $100,000 and up to five years in prison for obtaining protected health information under "false pretenses”
  - up to $250,000 and up to 10 years in prison for obtaining or disclosing protected health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.

Penn's High Level Approach to HIPAA

- Identify organizational components and communication links relevant to Health Care
  - Define which components of health information can be transmitted among which the components
  - Set up secure communication strategy among components (intranets, firewalls, encryption)

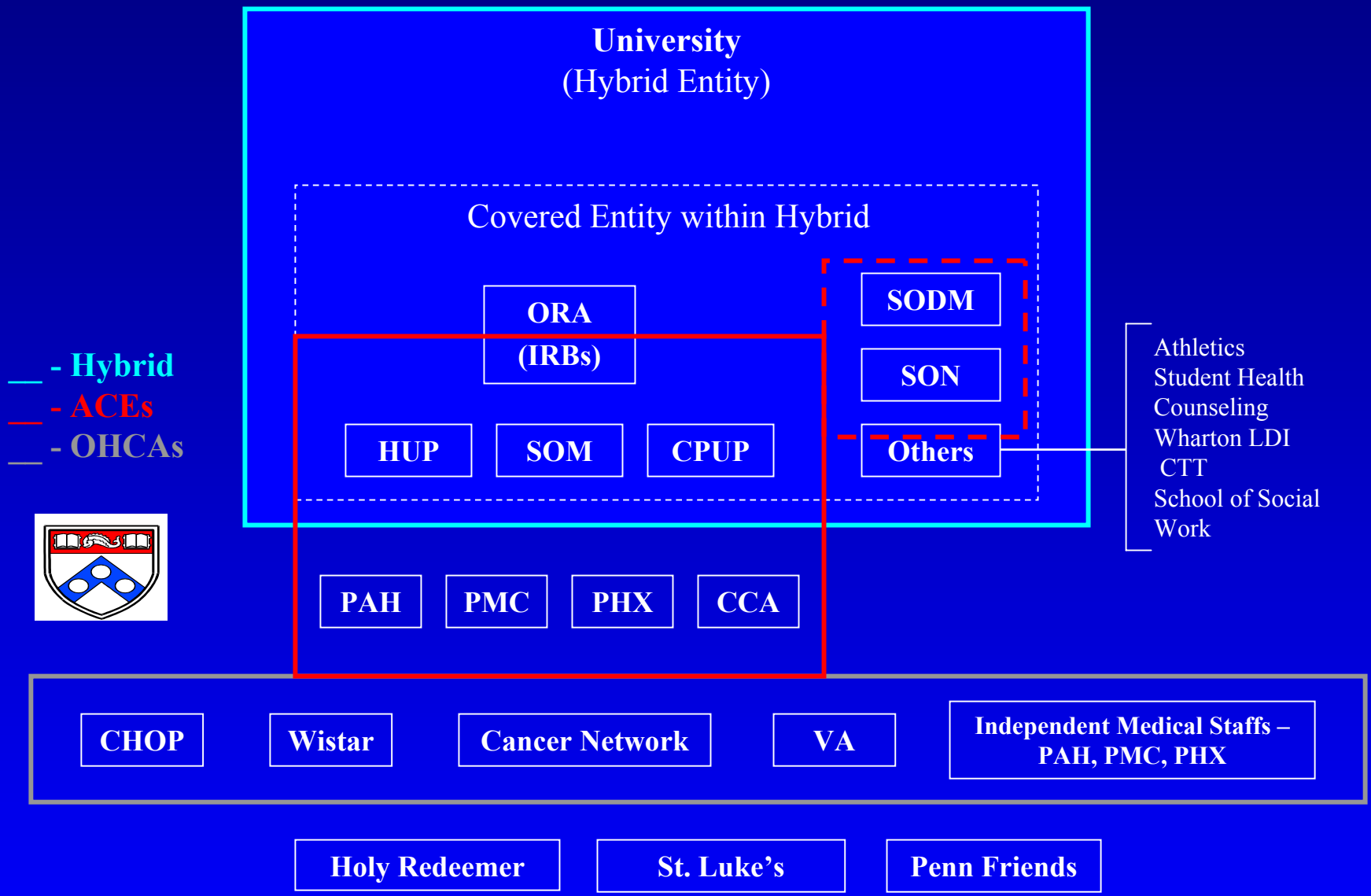
University of Pennsylvania Health System

- 4 owned hospitals
  - Hospital of the University of Pennsylvania
  - Presbyterian Medical Center
  - Pennsylvania Hospital
  - Phoenixville Hospital
- 65 owned primary care ambulatory practices (Community Care Associates)

University of Pennsylvania Health System

- Owned by the University of Pennsylvania that also has other related health care entities
  - Nursing school
  - Dental School
  - Student Health Service
  - Counseling

The overlapping lines of communication



Penn's Approach to Research Data Use

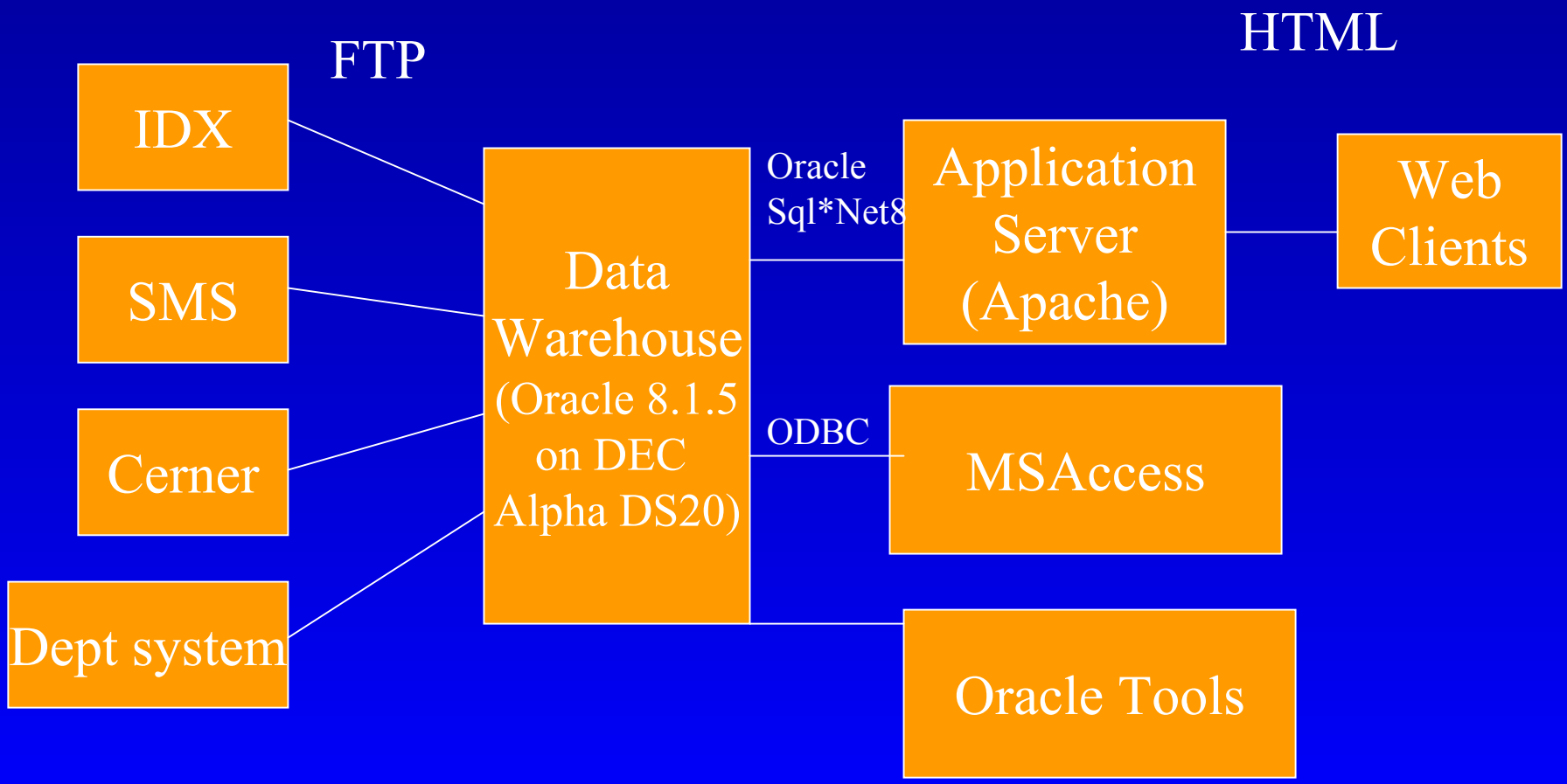
- Research requires data!
- Not all research requires personal identifiers
- Personal identifiers are often necessary to validate and integrate data from different systems
- Identifiers are often necessary to conduct retrospective research

Penn has a Research Database

- Pennsylvania
- Integrated
- Clinical and
- Administrative
- Research
- Database

} The PICARD System

Data Integration and Access



Available Data

- Ambulatory Data
  - Primary and subspecialty care data-- Jan 1997 - May 2001
  - Patient information
    - Location
    - Gender
    - Race
    - Birthdate
    - Insurance carrier

Available Data

- Inpatient data
  - Patient information
  - Admission Detail - 1988-1999 for HUP and Presby
    - Admission, DC dates, LOS
    - Diagnoses
    - Procedures for recent admissions
    - Charges for procedures/room/medicine etc.

Available Data

- Laboratory
  - 75 common chemistries, hematology and serology results since August, 1997
- Cardiology testing
  - Stress test, cath, echo results
- Pharmacy
  - Limited population
- Pulmonary Function test data

Penn's Approach to Research Data Use

- Minimal oversight
  - Information regarding a provider's own patients
  - Determination of numbers of patients meeting specified criteria
- IRB approval
  - Release of Medical Record numbers for additional chart review
- IRB and "PAC" review
  - Required before patient contact initiated

Administrative Issues in Data Use

- Steps to contact patients through a targeted approach for potential enrollment in research
  - Our office generates lists of potentially eligible patients
  - Lists forwarded to primary care provider (PCP)
    - Discretion if provider needs to contact patient
  - PCP returns lists of authorized patients to our office
  - Investigator receives list of authorized patients
  - Investigator contacts patients in the context of the PCP

Research Data Use vs Patient Contact

- Additional authorization from primary care provider required before contacting patients
  - Labor intensive process
  - Can we delegate responsibility for obtaining authorization to investigator?
  - Does patient have to be contacted by provider and affirm interest in study participation prior to being contacted by investigators?

Questions for discussion

- Should we allow patients to opt out of allowing their data to be used in research, even without personal identifiers?
- Do we allow patients to refuse directed contact regarding research participation? If so, for how long?
- Federal law vs. “6:00 news” law

Resources

- HIPAA Administrative Simplification:
  - http://aspe.hhs.gov/admnsimp/
- HIPAA Privacy:
  - http://www.hhs.gov/ocr/hipaa/
- Workgroup on Electronic Data Interchange Strategic National Implementation Process:
  - http://snip.wedi.org/
- American Association of Medical Colleges
  - http://aamc.org/members/gir/gasp