Privacy and Confidentiality

Brian C. Sauer, PhD

Veterans Affairs SLC IDEAS Center

University Utah Division of Epidemiology

Multiple Choice Question 1

- The only difference between a Limited Data Set and De-identified data is a limited data set requires a Data Use agreement for Research?
  - True or False
    - B. False
      - There are actually several differences between a limited data set and de-identified information
      - De-identified information must have all 18 elements removed
      - Limited data set does not require all 18 elements to be removed but it does require a DUA for research and public health reporting.

Multiple Choice Question 2

- Which of the following describes an approach to aggregating data from multiple owners while allowing owners/holders to maintain physical ownership and control over their protected data and their uses.
  - [A] centralized “all-payer” database
  - [B] centralized “cloud storage” database
  - [**C**] distributed network

Disclosures

- I have no financial conflicts relavent to this presentation.

- The following personal or financial relationships relevant to this presentation existed during the past 12 months/during the conduct of the study:
  - Employed by the Salt Lake City Veterans Affairs Medical Center
  - Employed by the University of Utah
  - Consulting: Consulted with Pfizer regarding an evaluation study of common data models.

Outline

- Defining Privacy and Security
- US Federal Regulations
- Important Concepts
- Role of IRB
- Data Protection
- State vs Federal
- International
- Examples
- Approaches to improve data access without

Tension Between Sharing Data and Protecting Privacy

- Acknowledgement of need to leverage data routinely collected during the delivery of health care to develop evidence about the safety and effectiveness of medical care
- Need to maintain person-level databases with the ability to link to external data sources while maintaining security and privacy of personally identifiable health information

A Regulatory Criteria for Approval

- Adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data exist
  - Privacy: refers to persons and their interest in controlling the access of others to themselves
  - Confidentiality: refers to the agreement between the investigator and participant in how data will be managed and used, i.e., the information is accessible only to those authorized to have access.

Balancing Act

- The need to keep personal information private is often weighed against the need to share personal information that has the potential to benefit the public good.
- The type of health information collected and used needs to be balanced against the risk of harm that could occur due to the unauthorized disclosure of that information.
- Balancing societal interests in research much be carefully considered by investigators and IRB and Privacy boards

Disclosure of Personal Information

- In limited circumstances personal information may be disclosed in the public interest without an individuals consent when benefits to society outweigh the individual's interest in keeping information confidential
  - Disease registration, communicable disease investigation,

Federal Regulations and Guidance

- The Belmont Report (1979)
  - Primary ethical statement guiding human research in the US and is the basis for our federal research protections
  - Three fundamental principles:
    - Respect for persons
    - Beneficence
    - Justice
  - Privacy and autonomy are are necessary to honor these ethical principles.

Federal Regulations and Guidance

- Code of Federal Regulations Title 45 part 46: The Common Rule
  - Defines human subjects as living individuals about whom a researcher obtains
    - Data through intervention/interaction with the individual or
    - Identifiable private information

Federal Regulations and Guidance

- HIPAA Privacy Rule: Relevance for Research
  - Supplements Common Rule by requiring covered entities to take specific measures to safeguard the privacy of individually identifiable Protected Health Information (PHI)
  - Covers participants consented for research as well as document or medical record databases, even if data were not generated from participants in research

Federal Regulations and Guidance

- Protected Health Information
  - List of 18 identifiers
    - Names, geographical identifiers, dates, phone numbers, fax, email, SSN, medical record numbers, health insurance number, account numbers, license, vehicle identifiers, device identifiers, URL, IP address, Biometric, photographic images, any unique identifying number, character or code except the unique code assigned by the investigator

Federal Regulations and Guidance

- HIPPA Disclosure of PHI
  - If research participants provide written **Authorization**
  - If Privacy Officer/Board has granted a **Waiver of Authorization**
  - If PHI has been **de-identified**
  - If **Limited Data Set** and **Data Use Agreement**
  - For research on **decedents** information if researcher provides required documents

Important Concepts Database Research

- Waiver of Authorization
- De-identified data
- Limited data set
- Data use agreement

Waiver of Authorization

- Possible when difficult or impossible to obtain written Authorization from research participants
  - Existing databases or repositories
  - When the research use of the health information does not represent more than minimal risk to privacy
  - Research could not be done without the requested health information

De-identified Data

- Exempt from HIPPA privacy Rule.
- Safe Harbor
  - De-identification requires the removal of the 18 PHI

Limited Data Set

- Protected health information from which certain specified direct identifiers of the individual and their relatives, household members and employers have been removed.
  - Name
  - Address
  - Phone number
  - Fax number
  - Email address
  - Vehicle ID
  - SSN
  - Medical record number
  - Health plan number
  - Account number
  - Certificate or license number
  - URL and IP addresses
  - Device ID
  - Biometric identifiers and full face images

Data Use Agreements

- Governs the sharing of data between an Information Custodian and a Requestor.
- Establishes the specific terms for VA and non-VA User uses.
- Provides a means to transfer liability for the protection of the information to an outside party.
- May serve as a means to establish criteria for using, disclosing, storing, processing, and disposing of data
- Must be implemented in accordance with policies established by Information Access and Privacy (IAP), and, if required, by the Information Custodian (IC).
- Satisfies HIPAA requirements when providing information within a limited data set (LDS)

Special Considerations/Protections

- Drug abuse programs
- HIV/AIDs
- Mental Health

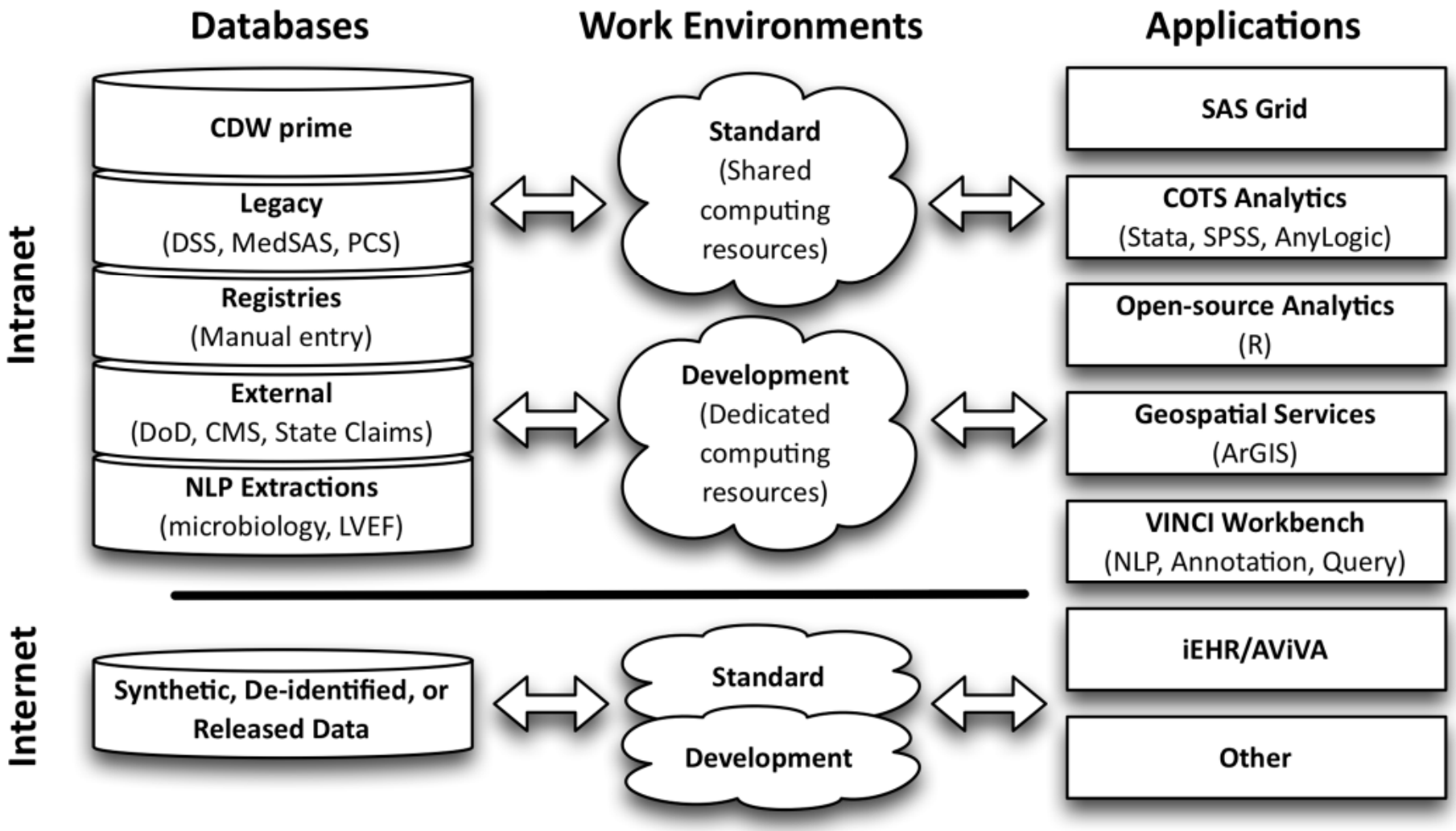
Role of IRB

- Designed to ensure that there are adequate provisions to protect the privacy of participants and to maintain confidentiality of data.
- Informed consent
  - Fair, clear, honest explanation of what will be done with information gathered about them
  - Promise of confidentiality cannot be absolute

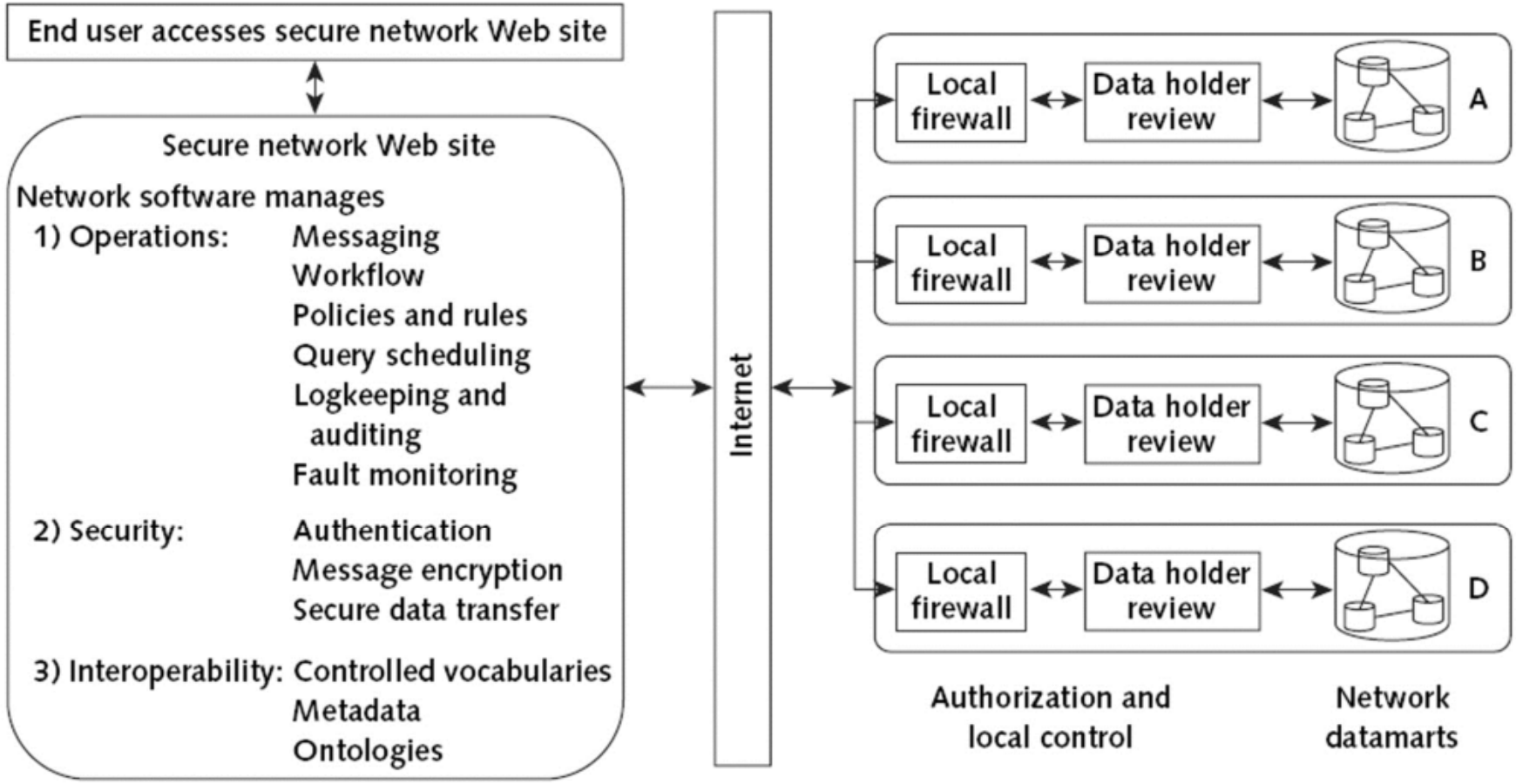
Data Protection

- Plans that state
  - who has access
  - measures for protecting the physical security and software security
  - authentication and authorization
- Data Architecture

VHA VINCI Centralized Cloud Storage



Design of a National Distributed Health Data Network



Ann Intern Med. 2009;151(5):341-344. doi:10.7326/0003-4819-151-5-200909010-00139