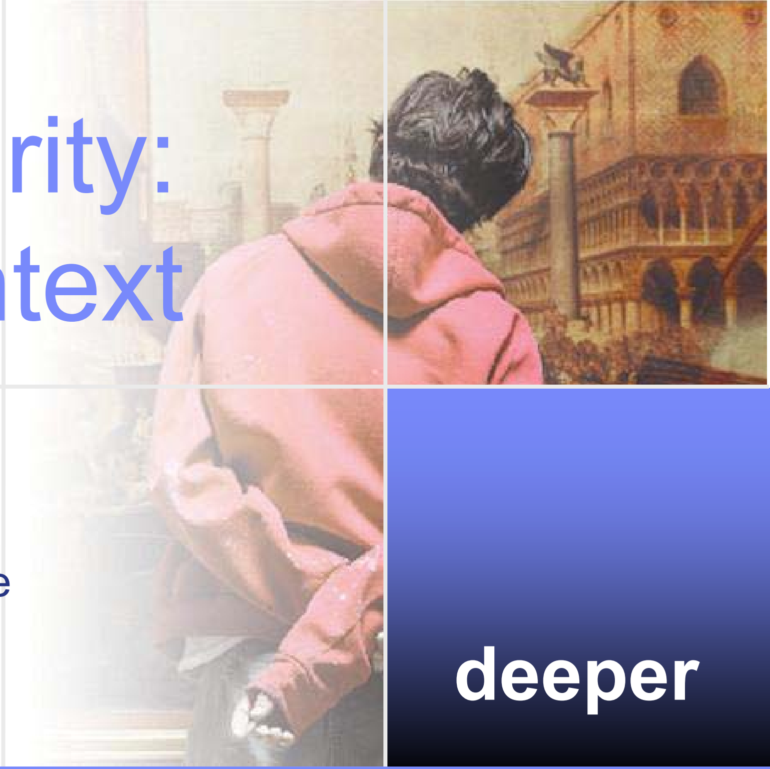
HIPAA Privacy & Security: Medical Research Context

HIPAA Summit Eight
March 9, 2004
Tom Hanks
Partner, Healthcare Strategy & Change
IBM Business Consulting Services
TomHanks@us.ibm.com
(312) 245-5917



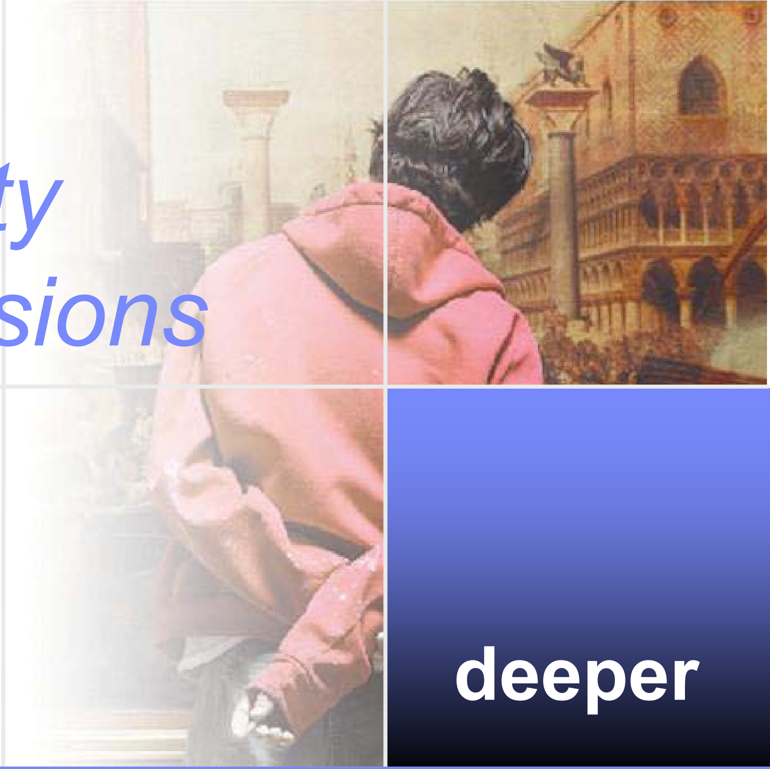
deeper

Using Research Databases Under HIPAA

- HIPAA Privacy & Security research specific provisions
- Special Challenges for Privacy and Security Implementations
- Architecture Solution Case
  - IBM Client Clinical Data Repository & Research Database
- Q&A

IBM Business Consulting Services

HIPAA Privacy & Security Research Specific Provisions



deeper

The Privacy Rule: Research Provisions

- Research means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.
  - (Definition from the ‘Common Rule’)
- Two forms of research are affected:
  - Research that only uses protected health information (PHI)
    - either with or without individual authorization.
  - Research that includes treatment of research participants.

Internal "Research" For Quality Activities

- Health care operations provision allows use of PHI for internal research conducted for quality assessment and improvement
- Must not be for purpose of generalizable knowledge – falls under general research provisions
- Study can begin for purpose of quality and convert to generalizable – but must be documented

Research Related “Covered Entities”

- Research organizations and investigators who do NOT perform patient care generally NOT covered entities
  - May be declared a covered entity in a hybrid organization – e.g. research organization owned by a university health system
- Researchers who provide treatment to research participants could be covered entities IF they conduct any of the named HIPAA transactions
- Researchers rely on covered entities (providers) to furnish research data

Using PHI for Research Purposes – Without Authorization

1. De-identified - safe harbor provision lists 18 data elements that must be removed
2. Limited Data Set – with Data Use Agreement
   - Adds full dates and full zip to a de-identified data set
     - E.g. - Could include 5 digit zip code, admit date, discharge date, dates of service, patient age, date of death
   - DUA establishes following terms to (1) identify users of LDS, (2) restricts further disclosure, (3) assurance of adequate safeguards, (4) report unauthorized use or disclosure, (5) promise not to identify information or contact individuals
3. IRB/Privacy Board waiver
4. Research protocol preparation
5. Deceased individuals

8 Waiver Criteria
(First 3 same as Common Rule)

1. Use or disclosure involves no more than minimal risk to the individuals;
2. Waiver will not adversely affect the privacy rights and the welfare of the individuals;
3. Research could not practicably be conducted without the waiver;
4. Research could not practicably be conducted without access to and use of the PHI;
5. Privacy risks are reasonable in relation to
   - the anticipated benefits, if any, to individuals, and
   - the importance of the knowledge that may result;
6. There is an adequate plan to protect the identifiers from improper use and disclosure;
7. There is an adequate plan to destroy the identifiers at the earliest opportunity, unless
   - there is a health or research justification for retaining the identifiers or if otherwise required by law; and
8. There are adequate written assurances that the PHI will not be reused or disclosed, except
   - as required by law,
   - for authorized oversight of the research project, or
   - for other research for which the use or disclosure of PHI would be permitted by the rules.

Minimum Necessary Provision

- Minimum necessary provision – limiting a researcher's access
- Specific to research[1], the HIPAA Privacy rule mandates providing and/or limiting access to protected health information (PHI) based on multiple parameters that include; (i) extent of PHI needed, such as a limited data set allowed for research purposes with a data use agreement[2], (ii) the purpose for which PHI is to be used[3], (iii) authorization by the patient[4], (iv) IRB waivers of individual authorization consistent with the common rule[5], and (v) if the individual is deceased[6],

[1] CFR 45§164.512(i)

[2] CFR 45§164.514(e)(1), CFR 45§514(e)(3), and CFR 45§514(e)(4)

[3] CFR 45§164.512(i)(1)(ii)

[4] CFR 45§164.508(c)(1)(v)

[5] CFR 45§164.512(i)(1)(i)(A) & CFR 45§164.512(2)(iv)

[6] CFR 45§164.512(i)(1)(iii)

Accounting for Disclosures of PHI for Research Purposes

- Accounting provisions apply for all disclosures NOT made under a valid authorization – e.g. IRB/
  - Date disclosed
  - Purpose of disclosure
  - Name of entity
  - PHI or classes of PHI disclosed
- PLUS + list of all protocols for which PHI may have been disclosed pursuant to an IRB waiver
  - Name of study or protocol
  - Purpose of study
  - Researchers' name & contact info
- AND - assist individual in contacting researchers

Accounting Not Required for Health Care Operations

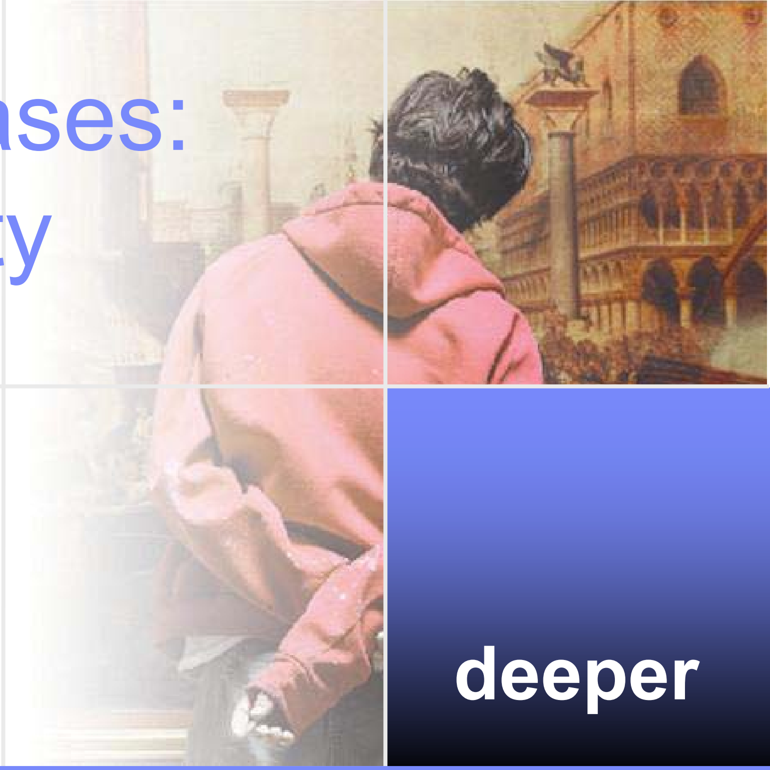
- Outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies.
- Population-based activities relating to:
  - improving health or reducing health care costs,
  - protocol development,
  - case management and care coordination,
  - contacting of health care providers and patients with information about treatment alternatives.
- Evaluating performance of providers and plans.
- Training programs.
- Accreditation, certification, licensing, or credentialing.

Individual Access

- Research participants have a right to access their PHI maintained in designated record sets, except:
  - If a covered entity is subject to CLIA and state law prohibits individuals from obtaining access;
  - If a covered entity is exempt from CLIA; i.e some research laboratories;
  - While a trial is in progress, if the individual has agreed, and has been informed that their right of access will be reinstated at the end of the research.
  - If research information is NOT in a designated record set.

IBM Business Consulting Services

Clinical Research Databases: Special Privacy & Security Challenges



Role Based Access Conundrum

1. Traditional role based access security controls provide a single “role” for each user that establishes that users ability to access data. Generally related to job function or “purpose” for access.
2. Researchers may need access to data for many different purposes and should be limited to accessing only the data appropriate for the specific purpose for which the user desires access
3. Role based access needs to be combined with purpose based access or presentation

Accounting for Disclosures

- Accounting for disclosure requirement for data obtained for research[1] is more stringent for research data that is obtained without patient authorization under an IRB Waiver.
  - Information related to the researcher who accessed the PHI must be retained. This includes (i) name of the protocol, (ii) description of the protocol, (iii) description of the type of information disclosed, (iv) the criteria for selecting the information (individual's record), (v) period of time the disclosures occurred, including the last time of disclosure, name, address and phone number of both the researcher and the research sponsor
- Mandate to assist patients in contacting researchers

[1] CFR 45§164.528(b)(4)

IBM

IBM Business Consulting Services

Case:
--Clinical Data Repository (CDR)

Special Challenges for Privacy and Security Implementations In Research Databases

deeper

Not an Everyday CDR - Goals and Objectives

- Provide a repository of clinical and genomic information to enable researchers to perform complex data mining activities
  - Identify disease behavior, protocol, and outcome patterns for further investigation
  - Locate disease and control cohorts for clinical studies
- Maintain wide range of clinical information, including MRI imaging, lab results, orders, observations, & outcomes
- Historical and current information
- Protect privacy of individual PHI consistent with Federal & State regulations

Enterprise IS/IT Strategy Alignment

- Security strategy moving forward
  - Strong authentication support future use of biometrics, tokens, etc.
  - Single-sign-on
  - Support LDAP/Active Directory
  - Overall identity management/protection
  - Auditing features of the CDR that may need to be consistent with internal audit requirements.
  - Web based platforms
  - Hosting and/or outsourcing
  - Network operations centers
  - CCOW support

Alignment With Clinical Information Strategy

- Direction of clinical standards adoption –
  - Standards used from data sources – multiple support with the CDR
  - LOINC
  - SnoMed
  - ICD-10 – Mortality now, moving to diagnosis and procedure
  - HL7 potential for transport between the CDR and source
  - Alignment with government standards initiatives – e.g. National Health Information Infrastructure (NHII) and Consolidated Health Informatics Initiative (CHI)

Clinician and Research Support Considerations

- Use of the CDR for clinical research not intended for generalization
- Tracking of IRB Consent/Waiver and/or individual HIPAA authorizations.
- Use of re-identification codes associated with de-identified health information – there are significant restrictions to the design and use of re-identification codes within the HIPAA Privacy rule.

Clinician and Research Support Considerations

- Coordination and expansion of data sources
  - Track researcher access to data and coordination of tracking disclosures with sources of data.
  - Automation of data loading – establishing filters and tracking of sources of data – automated transformation of clinical coding to standards
- Methodologies to obtain purpose for accessing the data and degree of authentication of purpose needed at the CDR user level.
  - Recording/tracking purpose for access
  - Accounting for disclosures

Clinician and Research Support Considerations

- Aggregate reporting design for de-identified reporting results of queries and data mining of PHI.
  - E.g. a query that defined the criteria of potential inclusion in a study. While the query would access PHI, the resulting report would be limited to supplying the number of individuals that met those criteria with a list of re-identification codes.
- Use of zip codes to determine geographic eligibility and candidate proximity to research facility – incorporating bureau of census data for calculation of zip code population to determine restrictions on usage.
- Tracking/auditing researchers' access to PHI and automation of reporting to individuals who are human subjects in studies.

Clinician and Research Support Considerations

- Purpose purpose code authentication against a separate, control database.
- Tracking of data use agreements, IRB Waivers & Consents, individual HIPAA authorizations.
- Maintenance of decedent information.

Summary of Security Access Control Criteria

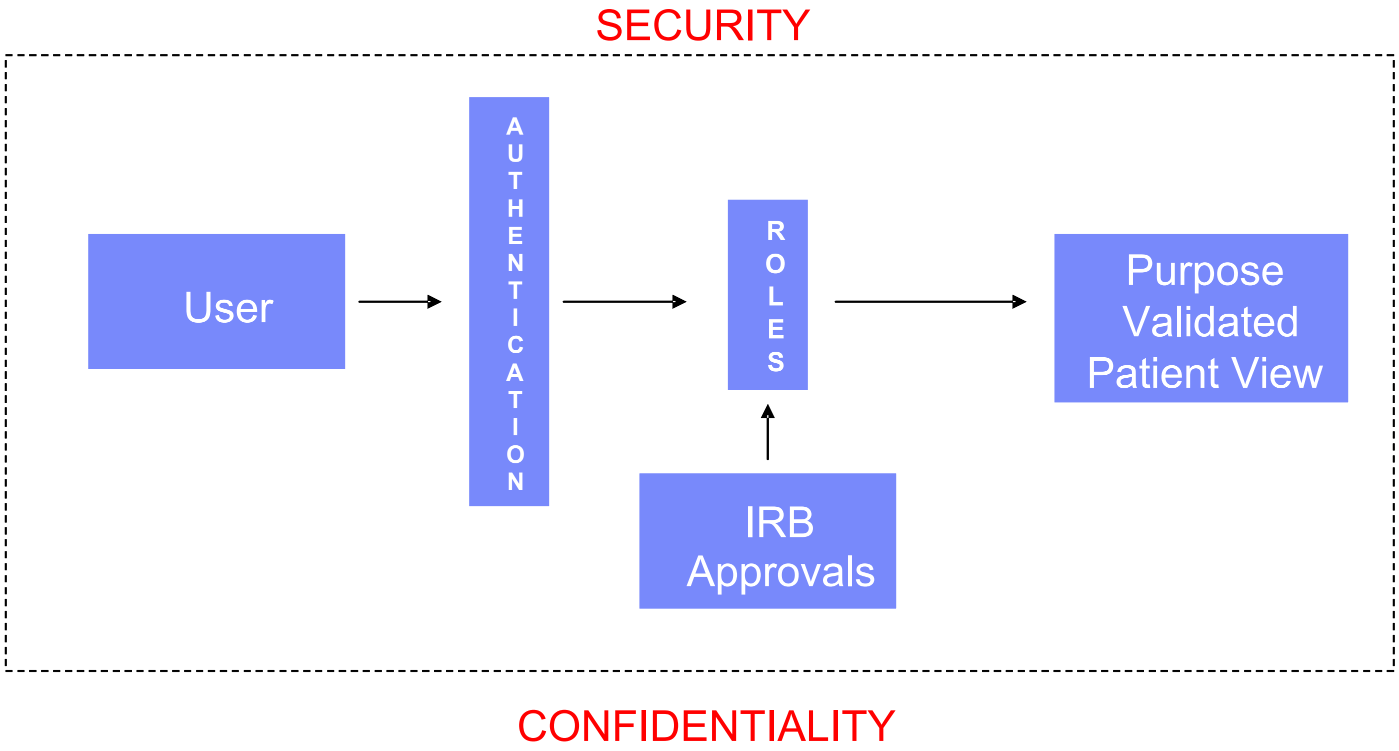
- Support multi-purpose data access and presentation for granting access rights to researchers, including categories of access (roles) and purpose of access. Ensure user transparent availability of data to researchers for;
  - For protocol development
  - Research on decedents
  - Use with clinical trial with and without history – separation of historical individual data from data gathered during trial.
  - Internal research for health care operations
  - With IRB Waiver/Consent
  - Limited data set under data use agreement

Summary of Security Access Control Criteria

- Aggregate reporting of data containing PHI into de-identified results
- Track access to data to support reporting of disclosures and assisting patients contacting researchers

Access Control Requirements

- Access to records containing PHI and access to specific PHI treated separately



Process Example (somewhat contrived)

- Principal investigator desires to undertake a clinical trial of “Supercalifragilistic Expialadocious” (SE) to ascertain the efficacy and safety of SE on human subjects suffering from Nanny’s Syndrome.
- The PI logs into the CDR and chooses the access purpose code for the review of clinical information to develop a research protocol.
  - For that purpose, CDR allows the PI to query and review information while on the physical site.
  - The PI is restricted from printing or downloading any data and is only allowed access to query and view CDR data while physically logged in to the CDR local domain.

Process Example (somewhat contrived)

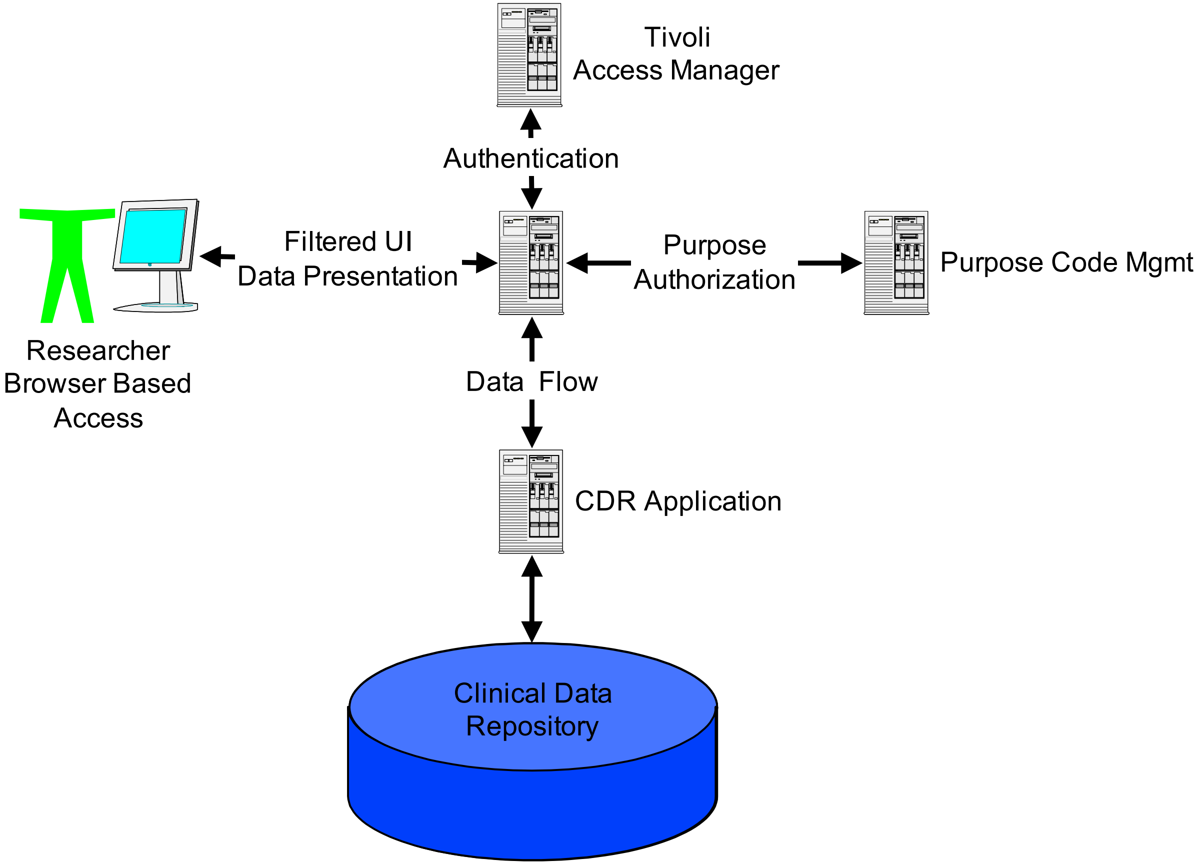
- After reviewing the available data, the PI has developed the criteria for identifying candidates for the proposed study and wants to determine if a valid cohort is available.
  - The PI chooses the purpose code for querying and delivering aggregate, de-identified reporting.
  - The IRB restricts the PI to performing queries against the data in the CDR and does not allow the PI direct access to the data itself.
  - Any reports resulting from the queries are reported in the aggregate without personally identifying elements (as defined in the HIPAA Privacy rule). E.g. These reports may provide information that lists how many subjects fit the PI's candidate criteria within a particular geography.

Process Example (somewhat contrived)

- Now that the PI has IRB Consent/Waiver, the PI requests that the re-identification codes be used to provide the demographic information for the candidates in order to seek their informed consent.
- In the meantime, armed with the IRB Waiver, the PI now has access to all of the cohort's individuals historical information to begin preparing baselines for the study.

Solution Architecture

Clinical Data Repository
Access Control & Privacy Management



CDR - Access Control Implementation

- Combine Tivoli Privacy Manager (TPM) with Tivoli Access Manager (TAM).
  - Reduces level of effort with developing security features with the CDR TAM and TPM are tightly integrated with Websphere access controls and keep security functionality from reducing the CDR performance.
- TAM provides user authentication for browser based access to CDR through its integration with Websphere
  - TAM supports role based access and uses an external LDAP database for provisioning
  - Support both local and remote access authentication and could be combined with a variety of strong authentication methods, including various biometrics.

CDR Access Control Implementation

- TPM separates the presentation of data from user authentication and granting of rights to access data. Provides a second layer of “purpose authentication” would be available and TPM could authenticate the user’s purpose to an external permissions database that contained the purpose codes, authorization history, protocol description, and so forth, maintained in conjunction with the IRB.
  - Forces the user to enter the purpose for access to the CDR.
  - Provides ability for user to access all data in all records for query and aggregate reporting purposes
  - Monitors all data being presented to the user and filters data before presentation to user to ensures that only the data consistent to the purpose for access is presented to the user

CDR Access Control Implementation

- Auditing and reporting capabilities track access to all PHI from all users and track the purpose for disclosure – fulfilling accounting for disclosure requirement to track and record access to PHI covered under an IRB waiver without individual authorization.

Questions?

Tom Hanks
Partner, Healthcare Strategy & Change
IBM Business Consulting Services
TomHanks@us.ibm.com
(312) 245-5917