

Compliance Challenges in Establishing and Using Clinical Databases

Melissa (Lisa) Thompson, JD, MPH
Adelman, Sheff & Smith, LLC

Betsy Hall, MPH, CHC
Director of Corporate Compliance,
Privacy and Information Security
Jewish Hospital & St. Mary's
HealthCare, Inc.

■ Melissa (Lisa) Thompson, JD, MPH

- Applicable law
- Database creation
- Protecting subject identity
- Future research purposes

■ Betsy Hall, MPH, CHC

- Operational considerations
- Breach examples
- Ramifications of non-compliance
- Enforcement
- Penalties

Regulation

- **HIPAA/HITECH**
 - Applies to individually identifiable health information created or maintained by covered entities/business associates
 - **Common Rule/NIH**
 - Applies to research conducted or supported by any component HHS, unless exempted under 46.101(b)
 - **FDA**
 - Applies to human research intended to support FDA pre-market submissions
 - **More . . .**
-

Regulation (continued)

- **Federal Alcohol and Drug Abuse Laws**
 - **Genetic Information - Genetic Information Nondiscrimination Act of 2008 (GINA)**
 - **Red Flag Rule**
 - **State Laws**
-

Research Definition

- Systematic investigation, including research development, testing and education, designed to develop or contribute to *generalizable knowledge*
- Includes development of databases for research
- Is this Research?
 - product manufacturer uses data from covered entity for in house research on product development

HIPAA/HITECH

- Health Insurance Portability and Accountability Act of 1996, Health Information Technology for Economic and Clinical Health Act (HITECH Act) in American Recovery and Reinvestment Act of 2009 and implementing regulations
- Applies to individually identifiable health information created or maintained by covered entities/business associates

HIPAA Privacy Rule – Use and Disclosure for Research

- De-identified data
- Limited data set (contains some PHI)
- Patient authorization for specific research protocol
- IRB/Privacy Board full or partial waiver of authorization
- Activities preparatory to research
- Research involving decedents
- Disclosure required by law
- Clinical trial recruitment
- “Grandfathered” research
- Restrictions on psychotherapy notes 42 CFR 164.508

HIPAA: Limited Data Sets (LDS)

- LDS contain PHI
- 16 categories of direct identifiers excluded
 - Name, zip code, vehicle plate numbers, full-face photos, SSN, telephone numbers, etc.
- May be used for research without obtaining patient authorization or IRB/privacy board waiver
- Data Use Agreement

HIPAA: Data Use Agreement for LDS

- Agreement between covered entity and recipient
- Establishes permitted uses and disclosures
- Further use/disclosure not allowed
- Additional stipulations
 - Appropriate safeguards must be used
 - Reporting disclosures to covered entity
 - Agents held responsible as well as entity
 - Cannot contact the individuals

HIPAA Activities Preparatory to Research

- Covered entity must obtain researcher representation
 - Use/disclosure solely to review PHI as necessary to prepare a research protocol or similar purpose
 - PHI will not be removed from covered entity
 - What about remote access - read only?
 - PHI necessary for research
- Researcher cannot contact prospective subjects under HIPAA unless either:
 - Covered entity workforce member
 - Business associate and BAA covers the activity
 - Waiver of authorization from IRB/Privacy Board
- Caution: Common Rule requires either 1) IRB approval and informed consent or 2) waiver

HIPAA Security Rule - EPHI

Administrative safeguards

- Privacy policies and procedures, training, emergency response, audits, handling security breaches
- Out-sourcing data to vendors for deidentification or creation of LDS – must ensure data protection

Physical safeguards

- Access, introduction or removal hardware/software, workstation use, contractor training

Technical safeguards

- Open network communications – encryption
- Data integrity, authentication (e.g., passwords, handshakes)
- Risk analysis and management programs

HITECH

- Direct HIPAA responsibility for business associates
 - Privacy and Security Rule requirements
 - Criminal and civil penalties
 - Responsibilities must be included in BAAs
- Breach notification requirements
- Accounting of disclosures
 - Includes disclosures for TPO when using EHR
 - 1/1/11 (EHR 1/1/09-1/1/11) or 1/1/13 (EHR before 1/1/09)
- Minimum necessary requires LDS if “practicable”
 - HHS to issue additional guidance that will supersede
 - Covered entity or business associate determines
- Increased enforcement

HITECH

- Restricts sale of PHI
 - Title of section: “Prohibition on Sale of Electronic Health Records or Protected Health Information”
 - Text: “shall not directly or indirectly receive remuneration in exchange for any protected health information.”
 - EHR => electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.
- Research exception – limitation on amount
- Exception for payments to business associates

HIPAA: Waiver or Alteration of Patient Authorization Requirements

- IRB or Privacy Board
- Full or partial waiver
 - Example: disclosing PHI for research recruitment purposes only
- No more than minimal privacy risk
 - Adequate plan to protect identifiers
 - Adequate plan to destroy identifiers (some exceptions)
 - Adequate written assurances PHI will not be reused or disclosed except permitted or required by law
- Research could not practicably be conducted without waiver/alteration
- Research could not practicably be conducted without access to and use of PHI

NIH/Common Rule

- Protection Human Subjects Regulations - 45 CFR Part 46 (Common Rule)
- Human subjects research
 - Individually identifiable data, includes obtaining information
 - IRB review required
 - Informed consent or IRB waiver of consent/authorization
- Not human subjects research
 - Data not individually identifiable and data for research not collected through interaction with subject
 - Informed consent and IRB review not required
- Exemption for collection or study of *Existing Data*, if publically available or recorded without identifiers or codes that can be linked back to subjects

IRB Waiver Under Common Rule

- IRB can approve full or partial waiver of informed consent
- IRB must find and document:
 - Research no more than minimal risk to subjects
 - Waiver will not adversely affect rights and welfare of subjects
 - Research cannot be practicably carried out without waiver
 - When appropriate, subjects will be provided with additional pertinent information after participation
- IRB waiver does not preempt other legal requirements for consent/authorization
- IRB waiver for public benefit/service programs

FDA Regulation

- Protection Human Subjects Regulations - 21 CFR Parts 50 and 56
- IRB and consent requirements
- Fewer exceptions

FDA Regulation:

IRB Review and Informed Consent

- IRB review required
- Informed consent required, unless one of emergency exceptions applies
- FDA guidance for in vitro diagnostic devices sets forth additional consent exception based on enforcement discretion
 - *Guidance on Informed Consent for In Vitro Diagnostic Device Studies Using Leftover Human Specimens that are Not Individually Identifiable (April 25, 2006)*

FDA Regulation: EHR

- FDA Scope and Reach
 - Software used with medical devices
 - Clinical decision-making support software
 - Certified EHR technologies
 - Examples: Telemedicine systems, wireless devices for patient monitoring
- Regulation – a work in progress
 - Proposed rule MDDS (medical device data systems)
 - Working group – which EHR systems FDA will regulate
 - 510(k) clearance process

Federal Law: Alcohol and Drug Abuse Records

- Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970
- Drug Abuse Office and Treatment Act of 1972
- 42 CFR Part 2

Federal Law:

Alcohol and Drug Abuse Records

- Patient identifying information may be disclosed for scientific research if program director determines that recipient of information
 - Is qualified to conduct the research
 - Has research protocol under which:
 - At least minimum security requirements met (42 CFR Part 2, section 2.16)
 - Patient identifying information is not redisclosed except back to program
 - Has met review requirements set forth in regulations, including protection of patient rights and risk/benefit analysis
 - Reports of research cannot identify patients
- Additional requirements in 42 CFR Part 2

GINA – Genetic Information

Nondiscrimination Act

- Genetic Information Nondiscrimination Act of 2008 (GINA)
- Applies to health insurers/group health plans

GINA – Genetic Information Nondiscrimination Act

- Research must comply with Common Rule and all other legal human subject protection requirements
- Clear indication that participation is voluntary and that non-compliance has no effect on enrollment or premiums or contribution amounts
- No genetic information collected or acquired as part of the research may be used for underwriting purposes
- Notify the Federal government in writing that it is conducting activities pursuant to this research exception and provide a description of the activities conducted
- Compliance with any future conditions that the Federal government may require for activities conducted under this research exception
- <http://www.hhs.gov/ohrp/humansubjects/guidance/gina.pdf>

Red Flag Rule

- Red Flag Rule 16 C.F.R. § 681.2
- Applies to “Creditors” with “Covered Accounts”
 - “Creditor” includes any entity that regularly defers payments for goods or services or arranges for the extension of credit
 - “Covered Account” is a consumer account that allows multiple payments or transactions or any other account with a reasonably foreseeable risk of identity theft
- Requires written Identity Theft Prevention Program
 - Identify the kinds of red flags that are relevant;
 - Explain your process for detecting them;
 - Describe how you’ll respond to red flags to prevent and mitigate identity theft; and
 - Spell out how you’ll keep your program current.

Database Creation

- NIH/Common Rule and FDA
 - ANY research purpose
 - Human subjects research triggers IRB/Informed Consent
- HIPAA/HITECH
 - PRIMARY purpose research
 - If primary purpose is TPO, then HIPAA research provisions do not apply to database creation, only subsequent research use.

Protecting Subject Identity

- HIPAA/HITECH
 - Strictest standards
 - Deidentified: identifiers listed in regulations eliminated or statistical testing – outside information relevant
 - Limited Data Sets with Data Use Agreements
- NIH/Common Rule and FDA
 - Not individually identifiable: identity of subject is not or may not be readily ascertained by investigator or associated with the private data

Protecting Subject Identity

- Deidentification
 - Health care operation
 - Business associate can perform – can be researcher – BAA required
- Limited Data Set with Data Use Agreement
- Database Filters
- Virtual patients
 - treatment intervals not dates, age not birthdates, etc.

Future Research Purposes

- HIPAA/HITECH
 - Patient cannot authorize unspecified future research use
 - Patient can authorize:
 - protocol-specific research use
 - storage in research database
 - disclosure to noncovered entity for future research
 - Deidentified or Limited Data Set
- NIH/Common Rule
 - IRB waiver of informed consent/authorization
 - Double-coded/deidentified with no researcher key
- FDA
 - IRB review required
 - Informed consent required unless guidance met on In Vitro Diagnostic (IVD) devices

Operational Considerations for Compliance

- Establish Policies and Procedures for Databases
- Establish a Centralized Database Registry
- Educate Investigators and Research Coordinators
- Monitor and Audit Clinical and Research Databases
- Establish mechanism for reporting research non-compliance
- Determine how to mitigate non-compliance
- Implement enforcement

Operational Considerations for Compliance

- **Establish Policies and Procedures for Databases that Address:**
 - When IRB approval is required for databases
 - When IRB approval is required to use data within a database
 - How to set up and use databases in compliance with federal and state privacy laws and regulations
 - Access controls
 - Physical and electronic security of protected health information (PHI) in the database
 - Consequences of non-compliance

Operational Considerations for Compliance

■ **Establish a Centralized Database Registry**

- Determine who should maintain the registry - Research Office, IRB, Compliance Office, etc.
- Require Investigators or Research Coordinators to submit information about the database during study approval process
- Mandate clinicians submit information about clinical databases prior to creation

Operational Considerations for Compliance

■ **Educate Investigators and Research Coordinators**

- On the facility's database policies and procedures
- About the federal and state privacy laws that govern databases
- When IRB approval is required
- On institutional, civil and criminal sanctions that have resulted from breaches of data

Operational Considerations for Compliance

■ **Monitor and Audit Clinical and Research Databases**

- Research Compliance Officer, Compliance Officer or the Privacy Officer should sample databases in the registry quarterly for compliance with:
 - Data Use Agreement – Are more identifiers being recorded than permitted under a Limited Data Set?
 - IRB approvals – Did the investigator get a waiver of authorization? If there is no waiver, are the appropriate HIPAA authorizations on file for each entry?
 - Privacy and Security regulations – Is the database physically and electronically secure? Etc.

Operational Considerations for Compliance

■ **Establish mechanism for reporting research non-compliance**

- Many options exist, including but not limited to:
 - Corporate Compliance Officer
 - Research Compliance Officer
 - Privacy Officer
 - General Counsel
 - Compliance Hotline
 - IRB
 - Study Sponsor

Operational Considerations for Compliance

■ Determine how to mitigate non-compliance

- Immediately stop what shouldn't be happening
- Protect patients/subjects from harm
- Follow reporting chain
- Work with Corporate Compliance Officer, Research Compliance Officer, Privacy Officer, General Counsel and possibly Public Relations on steps that need to be taken under federal and state privacy laws
- Take corrective action
- Report to patient (if required or decision is made to do so anyway)
- Report to any government agencies, IRB and sponsor if required

Operational Considerations for Compliance

■ Implement enforcement

- As part of corrective action, take any steps necessary to sanction those involved
 - Disqualify the investigator from conducting research at the institution going forward
 - Suspension or termination of the research
 - Disciplinary action against the investigator
 - Formal re-education
 - Assignment of a monitor
 - Require ongoing audits
 - Determine the data cannot be used for publication
 - Request publishers and editors be informed if data has been submitted for publishing or has been published

Operational Considerations for Research Compliance Programs

■ **Secure Clinical and Research Databases**

- House databases on secure network drives instead of hard drives, local drives or laptops
- Encrypt or password protect databases to prevent inappropriate access
- Limit access to those who have a “need to know”
- Use sophisticated databases that have audit trails
- Forbid storage on flash drives or external media (CDs, floppy disks) that are not encrypted or password protected
- Prohibit emailing databases
- Do not allow faxing of database information

Breach Examples – Stolen Laptop

- **February 2008** - A laptop containing medical information for 2500 people enrolled in a National Institutes of Health (NIH) clinical trial was stolen from the trunk of a car, putting patients at risk for medical identity fraud. The laptop contained **clinical trial data going back 7 years**, including names, medical diagnoses, and heart scans. The data was **not encrypted, despite government policies** that require this precaution.

Breach Examples – Server Hacked

- **September 2009** - University of North Carolina (UNC) School of Medicine in Chapel Hill notified about 236,000 women in a mammography research project that their Social Security numbers and other personal data may have been exposed when hackers breached the security of a database. The registry collects data from community-based mammography practices throughout North Carolina, and is part of a national mammography project funded by the National Cancer Institute. UNC sent notification letters to each person who may have been affected, along with instructions for actions they should take to protect themselves against the possible fraudulent use of their information.

Breach Examples – Inappropriate Disclosure

- **April 1998** - the daughter of a New Jersey physician - who agreed de-identified slides of his cancer cells could be used for research - received calls from colleagues offering their condolences after they saw her father's name in a computerized research database.

Ramifications of Non-Compliance

- **October 2009** – Wake Radiology, a multisite radiology group in central North Carolina that performs more than 650,000 procedures annually, decided it will no longer participate in studies that require patient information after UNC revealed that hackers breached the security of a mammography database.

Noting its “extreme concern about this occurrence,” Wake Radiology said that every file it sent to CMR was encrypted and password protected to protect patient privacy. The group added that it was awaiting information on the investigation that is being conducted by UNC officials.

Wake Radiology informed its patients that “involvement in future studies will be limited to anonymous, unidentified data.”

Operational Ramifications of Non-Compliance

- **HIPAA/HITECH**

- Document for HIPAA Accounting of Disclosures
- Possible Breach Notification
 - Individual patients
 - Media and HHS OIG within 60 days of discovery if more than 500 patients involved

- **NIH/Common Rule**

- Reporting privacy breaches to OHRP, the IRB that reviewed the study as well as the study’s sponsor if there was one

- **Red Flag Rule**

- Notify patients of privacy breaches involving social security numbers or financial information

Enforcement

- **HIPAA/HITECH**
 - HHS Office for Civil Rights for HIPAA
 - HHS Office of Inspector General for HITECH
 - State Attorney Generals
- **NIH/Common Rule**
 - IRB with oversight by OHRP
 - OHRP can require the covered entity to notify the individual(s) whose information was shared inappropriately. Such notification could cause the individual to file a complaint against the covered entity with OCR. That could lead to civil sanctions or criminal penalties under HIPAA. OHRP could revoke the investigator's data, prevent the investigator from publishing, suspend research indefinitely, or ban the investigator from conducting federally funded research in the future.
- **FDA**
 - FDA
- **Red Flag Rule**
 - Federal Trade Commission (FTC)

Penalties for Non-Compliance

- **HIPAA/HITECH**
 - Civil Monetary Penalties
 - \$100 per violation (capped at \$25,000 annually) for violations where the person did not know he/she committed a violation
 - \$1,000 per violation (capped at \$100,000 annually) for violations due to reasonable cause and not to willful neglect
 - \$10,000 per violation (capped at \$250,000 annually) for violations due to willful neglect and corrected within 30 days
 - \$50,000 per violation (capped at \$1.5 million annually) for violations due to willful neglect that were not corrected within 30 days
 - Criminal Penalties
 - Potential Lawsuits
- **NIH/Common Rule**
 - OHRP could revoke the investigator's data, prevent the investigator from publishing, suspend research indefinitely, or ban the investigator from conducting federally funded research in the future.
- **Red Flag Rules**
 - Civil Monetary Penalties
 - \$3,500 per violation
 - Injunctive Relief
 - Requires parties being sued to comply with law going forward; provide reports; retain documents and take other steps to ensure compliance with the Rule and the court order. Failure to comply with the court order could result in further penalties and injunctive relief.

Questions

Melissa (Lisa) Thompson, JD, MPH
Adelman, Sheff & Smith, LLC
(410) 224-3000
lthompson@hospitallaw.com

Betsy Hall, MPH, CHC
Jewish Hospital & St. Mary's HealthCare, Inc.
(502) 560-8404
betsy.hall@jhsmh.org