Accessing Electronic Health Record Data for Human Subjects Research: Challenges and Solutions August 2, 2012

Regulatory Challenges and Solutions

Mark A. McAndrew, J.D. (Taft)
Sara Simrall Rorer, J.D. (Taft)

<u>Panelists</u>

Katrina Trimble, J.D. (Privacy Officer TriHealth)
Mary J. Lopez, RN, J.D. (Privacy Officer UC, UC Health, UC Physicians)
Anthony J. Martin (Privacy/FOIA Officer, VA Medical Center)
Jeremy Corsmo, M.P.H. (Research Compliance and Regulatory Affairs, CCHMC)

Plan/Goals for Today's Presentation

- Overview of Key Regulations
- Panel Discussion/Roundtable – Applying those Regulations to Common Scenarios
  - How can the researcher(s) get/use patient data for research projects in compliant way?
  - Your Privacy/Compliance Officer is **not** your enemy!
    - Work with us! In most cases you can get the data you need.

Key Regulations – Confidentiality of Identifiable Patient Information

- FDA Informed Consent
- HHS (“Common Rule”) Informed Consent
- Health Insurance Portability and Accountability Act (“HIPAA”) Privacy Regulations ***

Key Regulations – FDA Informed Consent

- **FDA Rules apply to research involving drugs, devices, biologicals or other products under FDA control**
  - **As part of Informed Consent, FDA Rules require**
    - **A statement describing extent, if any, to which confidentiality of records will be maintained; and**
    - **A statement specifically noting the possibility that FDA may inspect research records.**
  - **In short, Informed Consent should make clear that when a subject participates in research, her records will be accessed by others, including specifically, the FDA.**
  - **The information that is given to the subject or the representative must be in language understandable to the subject**
  - **Do <u>not</u> require any specific confidentiality measures be taken.**

Key Regulations – HHS /Common Rule

- **Under HHS regulations "*research*" involves "*human subjects*" if an investigator (whether professional or student) conducting research obtains**
  - **data through intervention or interaction with the individual, or**
  - ***identifiable private information*.**
- **In turn, "individually identifiable" means the identity of the subject is or may readily be ascertained by the investigator or associated with the information**
- **Regulations not as detailed as HIPAA about "de-identification."**

Key Regulations – HHS /Common Rule (Cont'd)

- **Must comply with HHS Informed Consent requirements, unless exemption applies.**
- **<u>Key exemption</u>: "Research involving . . . existing data, documents, records, pathological specimens, or diagnostic specimens, if . . . the information is recorded by the investigator in such a manner that subjects cannot be identified, directly or through identifiers linked to the subjects."**
  - **This exemption would *not apply* if the investigators start with identifiable private information or specimens from existing records or specimens, and then record the data or information in a coded manner because the investigators (by their knowledge) have "keys" to the "code."**
- **Informed Consent (among other things) must include a statement describing the extent to which confidentiality of records identifying the subject will be maintained.**
  - **There is no requirement (unlike FDA) to specify that research records may be accessed by FDA or other Governmental representatives;**
  - **Gives IRBs flexibility to determine exact confidentiality measures needed for particular Study**
  - **As with FDA requirement, Informed Consent is supposed to be "in language understandable to the subject."**

Key Regulations – HIPAA

- **If your research requires you to create, use, or disclose patient information (or collect samples)**
  - **from healthcare providers' patients**
  - **Or third party "Business Associates" (Health Information Exchange) that use/collect patient information from those providers**
- **HIPAA will apply – in addition to (and frequently "trumps") FDA or HHS Rules**

Do the HIPAA Privacy Regulations Apply to My Research?

- **All "Covered Entities" must comply with the HIPAA Privacy Regulations**
- **Covered Entities include:**
  - **Health plans**
  - **Healthcare clearinghouses**
  - **Healthcare providers who transmit health information in electronic form**
    - **Doctors and their Practices**
    - **Hospitals and Clinics**
    - **Laboratories**
    - **Pharmacies (but *not* pharmaceutical companies)**
    - **Etc.**

Business Associates

NEW "HITECH" DEVELOPMENTS (effective 2/2010)

- **Key provisions of HIPAA now apply to a Business Associate (BA) in the same manner as the Covered Entity**
- **A BA is a third party that provides consulting, data management, other administrative services to Covered Entity**
  - **Health Information Exchanges are BAs (HITECH)**
  - **Must continue to have written BA Agreement**
  - **Don't know details until Regulations are published (way overdue)**

Basic HIPAA "Rule"

- A Covered Entity (or BA) may only use or disclose PHI as permitted by the Privacy Regulations
- Each Covered Entity (or BA) responsible for own HIPAA compliance, E.g.
  - TriHealth Hospitals (Good Samaritan Hospital & Bethesda North)
  - University Hospital
  - CCHMC
  - Separate Physician Groups (UC Physicians, TriHealth Physician Practices, independent Physician Practices (Wellington, Mayfield, etc.))
- Each Covered Entity may also be liable for its BA's non-compliance

How Do the Privacy Regulations Affect My Use/Disclosure of Patient Information?

Depends on:

- **What type of information will you use, collect, receive or release?**
  - **Is it Protected Health Information ("PHI") or "De-Identified"?**
  - **If it is PHI, what is the purpose for your use, collection, receipt or release? (KEY)**
    - **Does Physician (Investigator) need to use or disclose the PHI to treat her patient?**

      or

    - **For the case review that she wants to publish in a peer-reviewed journal?**

HIPAA Compliance

I am an individual Researcher (consultant for a BA) not a Covered Entity (or a BA) so why should I care about HIPAA Compliance?

Penalties For Noncompliance

- ***Covered Entities and Business Associates*** **subject to liability for HIPAA violations, under a 2-tiered system:**

  1. **Civil money penalties (4-tiers) (HHS)**

  2. **Criminal fines from $50,000 to $250,000, and receive 1-10 years in prison.**

Penalties For Noncompliance

- **4-Tiered System of *Civil* Penalties**
  - **$100 for per unintentional violation of HIPAA (aggregate cap: $25,000);**
  - **$1,000 per violation not "willfully negligent" (aggregate cap: $100,000);**
  - **$10,000 per willfully negligent but corrected violation (aggregate cap: $250,000)**
  - **$ 50,000 per willfully negligent, not corrected violation (aggregate cap: $1,500,000)**

Noncompliance

- **HITECH Changes to Criminal Penalty Provisions**
  - **Potential fines and imprisonment remain**
  - **HITECH now clarifies that individuals as well as Covered Entities (and Business Associates) subject to prosecution for violations.**
    - **Criteria: if the information is maintained by a Covered Entity (or Business Associate), and if the individual knowingly obtained or disclosed the information without authorization**

Administrative Rules – What Covered Entities Must Do

- Establish written policies and procedures (with respect to, among other things, the permitted uses and disclosures of PHI and patients' rights);
- Train all members of the workforce on the established policies and procedures (initially prior to the 2003 Compliance Date, upon new hires, and whenever significant changes in policies);
- Establish administrative, technical, and physical safeguards to prevent the unauthorized disclosure of PHI;
- Provide a process for patients to make complaints;
- Mitigate any known harmful affect arising from a violation;
- Refrain from intimidation or retaliatory acts (against Individuals for exercising their rights); and
- Refrain from requiring an Individual to waive the rights established by the Privacy Rules.
- Establish and apply sanctions against members of the workforce for violations;

PROTECTED HEALTH INFORMATION

- *What information is protected by HIPAA?*

Protected Health Information ("PHI")

Protected Health Information ("PHI"):

- **Is all "individually identifiable health information" prepared, transmitted or maintained in any form or medium, including paper, oral, or electronic, by the Covered Entity**
  - **The exact same "rules" apply regardless of the form of PHI**
  - **Example: if you need an "Authorization" to use (access) a patient's "paper" medical records for research, you need an Authorization to use a patient's EMR records for research, as well.**
- **Assume patient information is PHI unless "Deidentified."**

Protected Health Information (PHI)

- **In a hospitals and physician practices, PHI is:**
  - ***Everywhere***
  - ***In all types of formats – including verbal and electronic***
  - ***Includes information used (accessed), created, or disclosed by the hospital/practice***

HIPAA Pitfalls with EHRs

- **Ease of access to PHI in electronic form**
- **Access to PHI is easier to track electronically (i.e., electronic paper trail)**
- **BUT, many more access points exist**

HIPAA Pitfalls with EHRs

- ***Examples:***
  - University Medical Center in Tucson, AZ fired three support staff members who inappropriately accessed confidential EHRs of patients involved in the shooting of US Rep. Gabrielle Giffords.
  - In late 2010, the Mayo Clinic terminated two medical professionals, including a physician, who collectively accessed nearly 2,000 patient medical and financial records over a 4 year period.
  - In 2009, a doctor and two former hospital employees were prosecuted criminally and sentenced to a year's probation for accessing records of a murdered TV newscaster.

HIPAA Pitfalls with EHRs

- ***More examples:***
  - University of Iowa Hospital and Iowa City clinics fired three employees and disciplined two others after discovering that they inappropriately accessed the EHRs of 13 University of Iowa football players.
  - UCLA Medical Center found that at least 127 employees had improperly accessed the medical records of celebrities. One employee was indicted in 2009 for purposefully removing certain information and for recording Farah Fawcett's medical records.

HIPAA Pitfalls with EHRs – How to Protect the Institution

- Conduct risk assessment
- Appropriate training and policies/procedures for responding to inappropriate uses or disclosures
  - Consistent enforcement – zero tolerance?
  - Alignment with HR Department
- Test files?
- CMS enforcement actions indicate that institution or facility can avoid liability if actions result from rogue staff despite appropriate policies/procedures in place

HIPAA and Research

- **General Rule**: An Authorization will be required before a researcher may use (access) or disclose a hospital's (or physician practice's) patient **for research purposes**, unless an exception applies

Example – What's the purpose of the use/disclosure of PHI?

Physician needs to review a patient's office medical records (from her own Medical Practice), and her hospital records from Hospital #1 related to a surgery performed on a particular patient two years ago, in order to prepare for an upcoming surgery at Hospital #2 next week. What does Physician need to do to receive and review these records?

PERMITTED USES AND DISCLOSURES OF PATIENTS' PHI (PTO)

PAYMENT…TREATMENT…OPERATIONS

- ***Also known as "PTO"***

  By far the most frequent and "routine" uses/disclosures of PHI by healthcare providers –

PERMITTED USES AND DISCLOSURES OF PATIENT'S PHI (PTO)

- **No Consent/Authorization Required**

- **PHI may be disclosed/used for own PTO purposes, as well as the PTO purposes of another Covered Entity. Example:**

  - **Family Physician sends information (orders, etc.) to Specialty Physician to facilitate care ("treatment" purpose)**

  - ***Note: except for "treatment" uses/disclosures, HIPAA's "minimum necessary" standard applies***

Uses or Disclosures of PHI for Treatment Purposes

Physician may access the records (EHR or "paper")

- from her own practice (one Covered Entity)
- and each Hospital (separate Covered Entities)
  - Without the patient's written or verbal Authorization, consent or permission.
  - If on EHR, will have to work out access arrangement

PHI Uses and Disclosures for Operations Purposes

What about teaching residents/students?

- Physician's use/disclosure of patient's medical information also is permissible for educating residents, fellows, interns, or other student health care professionals that she is currently teaching/supervising, as part of the **Health Care Operations** of the those hospitals actively participating in residency/training programs).
  - Disclosures subject to "minimum necessary" rule (must limit individually identifiable information to the minimum necessary for the teaching purpose)
  - For EHR systems, need to work out access arrangement with each Entity

Health Care Operations (Definition)

Includes:

- Quality assurance and improvement activities and studies, including development of clinical guidance (but not if obtaining "generalizable knowledge" from the study is primary purpose)
- Evaluating practitioner/provider competence and conducting training programs for healthcare practitioner who learn under supervision to practice or improve their skills
- Conducting or assigning for medical or legal audits and compliance programs
- Business management, administration, and development activities

But *does not* include*: RESEARCH*

Example – What's the purpose of the use/disclosure of PHI?

Several months after the Surgery and follow up treatment, Physician decides that Patient's condition would make a very interesting Case Study for publication in a nationally-circulated journal. What steps must Physician take to ensure that she complies with HIPAA?

"Operations" Use or "Research" Use?

- The **purpose** behind Physician's use is the key to compliance
  - This probably ***is not*** use or disclosure for "PTO" purpose (or is it)?
    - ***Panel -- Discuss***
  - If published case study is "research" for HIPAA purposes, even if the Case Study will be "de-identified" in final published form, Physician's access/review of patient's PHI in preparation of the case study *prior to* its de-identification, constitutes a HIPAA "**use**" for research purposes
- **General Rule**: An Authorization will be required before the researcher can use or disclose patient's PHI for research purposes, unless an exception applies.

Research

For HIPAA purposes, research is defined broadly:

A systematic investigation, including research development, testing and evaluation designed to develop or contribute to "generalizable knowledge"

SIDE NOTES……

- ***Key points:***
  - **Research is not "<u>treatment</u>" for HIPAA purposes**
  - **Research is not "<u>healthcare operations</u>" for HIPAA purposes**

The HIPAA Research Authorization – Points to Remember

- An Authorization will be required if there will (can) be ***contact*** with the research subject (i.e., this is a current patient)
- The Authorization may be combined with the informed consent document or kept separate as a stand-alone document
  - However, a Hospital may have own policy requiring a separate Authorization
  - *DISCUSSION: What are Panelists' institutions' doing?*
- Other contemplated uses or disclosures should be set forth in the Authorization as well (e.g., FDA and other Governmental Inspections, Sponsor/CRO Study monitoring, publications, etc.)

HIPAA Authorization for Research – Requirements

- **An Authorization for Research must contain very specific core elements and required content**
  - **Your Privacy Officer or IRB can likely provide sample HIPAA Authorizations developed for your Organization**
- ***Can* condition participation in Study (but not ongoing treatment) on willingness to sign Authorization**
- ***Currently*, an Authorization may only be used for 1 specific Study**
  - **Must obtain *separate Authorization* (or comply with exception) for *future research*, example:**
    - **Creation of Data Base (Study #1 needs Authorization #1)**
    - **Future research use of that Data Base (Study #2 needs Authorization #2)**
- ***Proposed* HIPAA Regulations would permit combining current and future research into 1 Authorization**
  - ***??? FINAL***
  - ***Understandable?***

Exceptions to the Rule that an Authorization is Required to Use/Disclose PHI for Research Purposes

- **Activities Preparatory to Research *****
- **Research on Decedents' Information**
- **Research Using De-Identified Information *****
- **Research involving a Limited Data Set** where there is a valid Data Use Agreement in place
- **IRB (Privacy Board) Waiver or Alteration of the Authorization requirement *****

Exception to the Authorization Requirement – Activities Preparatory to Research

HIPAA allows researchers to access information without an individual's Authorization for activities preparatory to research when the researcher provides the Covered Entity with a written statement containing the following:

- The researcher represents that she seeks access to the PHI *solely* to prepare for research;
- The researcher states that the PHI is necessary for research purposes; and
- The researcher represents that PHI ***will not*** be removed from the Covered Entity in the course of the review.

- ***Panel:***
  - ***Can you "remotely" access Hospital's EMR?***
  - ***What procedures (forms) does your organization require?***

Exception to the Authorization Requirement – Activities Preparatory to Research, or Not?

- **Scenario**: A private practice physician who also was PI of a study disclosed a list of patients and diagnostic codes to a CRO to contact patients for recruitment purposes.
  - Enforcement action brought against physician practice for wrongful disclosure.
- **Response**: Private practice maintained that the disclosure to the CRO was permissible as a review preparatory to research.

Exception to the Authorization Requirement – Activities Preparatory to Research, or Not?

- **CMS Finding**: Activities considered "preparatory to research" include preparing a research protocol; developing a research hypothesis; and identifying prospective research participants.
  - Researcher may not remove PHI from the covered entity for purposes of contacting potential study recruits.
- **Remedy**:
  - Revision of practice policies and procedures to permit disclosure to an outside researcher for research recruitment, only if a valid authorization is obtained from each individual or if the covered entity obtains documentation that an alteration to or a waiver of the authorization requirement has been approved by an IRB or a Privacy Board.
  - Training of all physicians and staff members on the new policies and procedures.

Exception to the Authorization Requirement – Activities Preparatory to Research, or Not?

- **Scenario 2**: Outpatient surgical facility disclosed a patient's PHI to a research entity for recruitment purposes without the patient's authorization or an IRB or Privacy Board approved waiver of authorization.
- **CMS Finding:** Covered entities seeking to disclose PHI for research recruitment purposes must obtain either a valid patient authorization or an Institutional Review Board (IRB) or privacy-board-approved alteration to or waiver of authorization.
- **Remedy**:
  - Revision of practice policies and procedures to permit disclosure only if a valid authorization obtained and training of all physicians and staff members on the new policies and procedures.
  - Log the disclosure of the patient's PHI for accounting purposes.
  - Send patient apology letter for the impermissible disclosure.

IF IT'S NOT PHI

- DE-IDENTIFIED DATA MAY BE USED FREELY
  - (WITHOUT ANY HIPAA RESTRICTIONS)
- FOR **ANY** PURPOSE – INCLUDING RESEARCH

PHI

SOURCE: PATIENT MEDICAL RECORDS OF THE HOSPITAL/PRACTICE		Checklist:
Record No. 0012345 Name: Penny Patient Address: 1234 Highland Ave Cincinnati, OH 45219*	Date of Birth: 12/05/60 Gender: Female Physician: Dr. M	Covered Entity? Yes No Individually Identifiable? Yes No Health Information*? Yes No
Diagnosis: *Aneurysm* Treatment: [Summary of prior and current surgeries and hospitalizations, tests, office visits, etc]		
*PHI includes demographic information about an individual.		

DE-IDENTIFICATION - "Safe Harbor"

Removal of These Identifiers Makes Information De-Identified	
Names	Account #s
Addresses (including city and ZIP)	Certificate/license #s
Elements of dates (except year)	VIN and Serial #s, license plate #s
Ages over 89 years	Device identifiers, serial #s
Telephone #s	Web URLs
Fax #s	IP address #s
E-mail address	Biometric identifiers (finger prints)
Social Security #	Full face, comparable photo images
Medical record, prescription #s	Unique identifying features
Health plan beneficiary #s	
Health information is de-identified if the above identifiers of the individual or of relatives, employers, or household members of the individuals are removed *and the Covered Entity has no actual knowledge that remaining information can be used, alone or in combination with other information, to identify the individual.*	

DE-IDENTIFIED INFORMATION

SOURCE: PATIENT MEDICAL RECORDS OF THE HOSPITAL/PRACTICE		Checklist:
Record No. Name: xxxxx Address: 452xx	Date of Birth: /60 Gender: Female Physician: Dr. M	Covered Entity? Yes No Individually Identifiable? Yes No Health Information*? Yes No
Diagnosis: *Aneurysm* Treatment: [Summary of prior and current surgeries and hospitalizations, tests, office visits, etc BUT MUST TAKE OUT ALL DATES, INCLUDING DATES OF SERVICE]		

NOTE: If the Covered Entity has actual knowledge that remaining information can be used to identify the individual, the information is considered individually identifiable, and therefore, generally is PHI.

DE-IDENTIFICATION - Alternative

- Privacy Rule permits “de-identification” through a “statistical method.”
  - A qualified statistician determines that the method used will render the information as not individually identifiable, and that the risk of “re-identification” is very small.”
  - Statistician must document methods and results that justify his or her determination.
  - ***Panel: Anyone using/working toward “statistical method?”***

STATISTICAL DE-IDENTIFICATION – Key Considerations

- Find a qualified expert
- Risk of re-identification does not need to be eliminated
  - Analysis only required to show that risk is “very small”
- What information is “reasonably available” from external data sources that could be used to re-identify disclosed information?

STATISTICAL DE-IDENTIFICATION - Key Considerations

- Does inclusion of certain dates in information to be disclosed add to re-identification risks?

- Dates of service: inclusion of dates of service (more specific than the year) may be permissible because it may not add to risk of re-identification
  - Date of service not generally available in external databases with other identifying information, and therefore may not be considered "readily available information"

- Contrast with date of birth and date of death, which may be matters of public record and therefore would constitute "readily available information"

STATISTICAL DE-IDENTIFICATION - Key Considerations

- Data Use Agreement (DUA) may provide additional comfort to parties.

- Prohibit recipient from re-identifying, or attempting to re-identify, any patient or individual (or relative or family member) that is the subject of the disclosed information.

Limited Data Sets

- **Under Privacy Rule, "Limited Data Set" may be used/disclosed for research purposes without authorization or IRB Waiver**
- **Strips data of most identifiers, but leaves in --**
  - **Zip codes and other geographic information (but not street or address)**
  - **Any dates directly related to patient (e.g., birth date, admission date, discharge date, treatment dates)**
- **Disclosing and receiving entities must enter into a "Data Use Agreement" limiting use/disclosure of the limited data set for the specified research.**

Panel: What's Your Experience?

IRB/Privacy Board Waiver of the Authorization – Specific Requirements

- Before disclosing PHI pursuant to a IRB or Privacy Board waiver of Authorization, a Covered Entity must obtain the following documentation from the IRB or Privacy Board:
  - Signature and date of written waiver
    - The waiver must be signed by the chair (or other member) of the IRB or Privacy Board
    - The waiver must indicate the date on which the IRB or Privacy Board approved the waiver of Authorization
- Review Procedures—a statement from the IRB or Privacy Board that the waiver has been reviewed and approved under either normal or expedited review procedures
  - The IRB must follow the requirements of the Common Rule in determining whether to conduct normal or expedited review procedures to approve the waiver

IRB/Privacy Board Waiver of the Authorization – Specific Requirements (continued)

- **Required Criteria**
  - The use/disclosure of PHI involves no more than minimal risk to privacy based on an adequate plan to protect the individual's identifiers
  - The plan to protect the identifiers must include written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research permitted by the regulations
  - ***The research could not practicably be conducted without the waiver or alteration of the Authorization requirement***
    - ***If you have/can have contact with patient and can get the Authorization criteria NOT met.***
  - A brief description of the health information the IRB or Privacy Board has determined is necessary for the research

Suggestions for Researchers Coping With HIPAA:

- Allow ***time*** to plan/adjust for HIPAA Compliance
  - You probably can get the patient data you need, but getting the Authorizations (or following the IRB Waiver or other exceptions) will take time
- When possible, create and/or use ***De-Identified Data***
  - The earlier in the research process the better
- Remember, all "research" uses ***prior to*** De-Identification require Authorizations (or a fit within an exception -- IRB Waiver, Preparatory to Research, Decedents' PHI, etc.)

- ***PANEL DISCUSSION/QUESTIONS????***


Taft