The Use of Patient Records (EHR) for Research

Mary Devereaux, Ph.D.
Director, Biomedical Ethics Seminars
Assistant Director, Research Ethics Program & San Diego Research Ethics Consortium
Abstract

The growing availability of electronic medical records, and large databases of health information such as EPIC, afford researchers a range of opportunities. Computerized searches of large troves of de-identified patient medical information promise a better understanding of disease patterns, treatment efficacy, and the contribution of genetic and other factors in health. These possibilities, however, raise a number of ethical, legal, and regulatory challenges.
Challenges

• What does de-identification mean?
• Can it be done, and with what assurance?
• Do patients own their medical information — with the right to refuse consent for its use — or is such information a shared social resource available to all?
• What are the responsibilities of biomedical researchers using EHRs and what does the IRB require?
Aims

• To outline ethical challenges in gathering, accessing, and using personal patient information for non-clinical purposes, i.e., “secondary use”
• To understand the risks and benefits of secondary use of patient data
• To apply principles of medical ethics to medical informatics, e.g., research with aggregate patient data and/or data mining
• To discuss how best to meet these challenges, protecting patient rights and promoting research access.
First, two distinctions

- Research vs. Patient care
- Primary vs. Secondary Use
Research vs. patient care

Key distinction
Original Use: Patient care

- Clinicians gather personal patient information to prevent, diagnose and treat disease and advance patient health.
  - Collection of data
    - Family history
    - Lab tests
    - Record of procedures
    - Insurance status
    - Compliance, e.g., prescriptions filled
    - What else gets collected?
Secondary Use

• Defined as
  ▫ “Non-direct care use of personal health information (PHI) including but not limited to analysis, research, quality/safety measurement, public health, payment, provider certification or accreditation, and marketing and other business including strictly commercial activities.”

Examples of Primary vs. Secondary Use

- Dr. Welby, a community pediatrician, keeps meticulous records on his patients, including data on infant height, weight, and head circumference; immunizations, and so on. She instructs the office nurse to call patients whose children are due for physical exams or vaccinations.

- A university research team designs and receives IRB approval and funding for a study of emergency medical treatment across the US. They approach the Center for Disease Control and Prevention and “request a scrubbed copy of the agency’s BioSense data.” Safran et al. 2007
## Challenges of replacing paper records

<table>
<thead>
<tr>
<th>Paper Records</th>
<th>Electronic Medical Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>One record</td>
<td>Many copies</td>
</tr>
<tr>
<td>One place</td>
<td>Stored here, there, cloud</td>
</tr>
<tr>
<td>Limited access</td>
<td>Easy to access</td>
</tr>
<tr>
<td>Relative ease of control</td>
<td>Security risks high</td>
</tr>
<tr>
<td>Limited usefulness</td>
<td>Extreme usefulness</td>
</tr>
</tbody>
</table>
Familiar Arguments for EMR

• Benefits
  ▫ Improved healthcare delivery
  ▫ Consistent care across providers
  ▫ More access and control
  ▫ Greater efficiency and lower cost
  ▫ Research possibilities of EPIC, national databanks, international databanks
Value of Aggregated Health Data

- Large scale studies of disease trends, public health, outcomes, etc.
  - Expand basic knowledge
  - Improve patient care
  - Increase healthcare system safety and efficiency
  - Lower costs
  - Documenting inequities in care or reimbursement
  - Other?
But also challenges. . .
Familiar issues

PRIVACY

SECURITY
Privacy

• Who has control of what goes into the record?
• Who has access?
• Who should have access? In what circumstances and for what purposes?
• What penalties for breaches?
• HIPAA limitations
  “covered entities” may disclose de-identified patient information
Patient Data Protections

- Like the rest of clinical medicine, record keeping governed by principles of medical ethics
  - Respect for persons/autonomy,
  - Beneficence (do good and minimize harm),
  - Justice (treat fairly)

- Also protected by professional guidelines and the law
  - Right to privacy - includes medical records
  - Professional guidelines regarding patient confidentiality
  - HIPAA Privacy Rule re: research
Updated HIPAA Authorization

- As of September 23, 2013, newly enrolled participants who need to sign a HIPAA authorization must "opt-in" to allow the use of their PHI for optional sub-studies and future secondary use of personal health information (PHI).
  - The HIPAA authorization has been updated to include a checkbox to indicate that the participant has agree to allow information to be disclosed for the additional optional research activities explained in the informed consent process.
  - http://irb.ucsd.edu
Secondary Use of Existing Data

• Requires IRB Approval or Certificate of Exemption

• Reminder: Investigators and study staff are reminded that the secondary use of existing data/specimens, including review of existing medical records, student records, accessing computer databases that have been produced from previous studies, etc., requires IRB approval or Certification of Exemption from IRB review.
  ▫ http://irb.ucsd.edu
Technical Protections

• Is technology the solution?
• Other means of ensuring privacy
  ▫ De-identification
  ▫ Encryption
  ▫ Controlled access
  ▫ Other technical strategies/tools?
• Necessity for re-identification for some research uses undermines “promise of anonymity”
Security

- Is any system *really* safe?
  - Cost
  - Quality of system installed
- Why do we care about security?
- What’s the big deal about privacy?
  - For patients
  - Doctors
  - Society
Beyond Privacy & Security
AMIA Identified Issues

- Public awareness and trust
  - Patients, providers and larger public unaware of benefits and risks of secondary use
- Ownership and access
  - “Who owns health data and who has the right to access and for what purposes?”
- Control
  - “Do patients have the right to audit or put other health constraints on the use of their data, even after anonymization?”
Public awareness and trust

- Dr./patient relationship based on confidentiality
- Secondary use is widespread, but “providers, physicians, and their patients are generally unaware of this development. . .”
  - Safran et al, p. 5
AMIA Recommendation 1

• Transparent policies and practices for a start
  ▫ Policies may need to be updated as technology evolves through data life cycles.
  ▫ Acknowledge complexity of process
  ▫ As re-identification of patients remains a possibility, various stake holders need a place at the table.
  ▫ “Ongoing public policy discussions must explicitly and directly address the secondary use of health data.”
Increased Transparency

- Consumers willing to share private information for health research
  - Small 2010 Boston study showed support for sharing, especially among the young, healthy, and students, or during public health emergencies
  - Willingness increased with anonymity, research use, engagement with a trusted intermediary, transparency, and payment.
Recommendation 3, 4

- Discussion and consensus building
- Increase public awareness with public education
- Create taxonomy of secondary uses of health data “to clarify societal, public policy, legal, and technical issues.”
Discussion
Ownership and Access

• Secondary use of private patient information poorly monitored.
  ▫ **Patients may have reason to worry**

• Should we adopt “opt in” rather than “opt out” models?

• Should patients have the right to control what information goes “public” and for what use?

• Is such a system technically and practically feasible?
Control

- If my information is acquired with my consent and de-identified and held securely, do I have any further rights over what is done with it?
  - Do I have the right to audit my information? May I specify for what kind of research it may be used?
    - Curtailing insurance benefits?
    - Developing programs of bioterrorism?
    - Publishing community health profiles?
Sources

• Sharing Medical Data for Health Research: The Early Personal Health Record Experience, Elissa R Weitzman, Liljana Kaci, and Kenneth D Mandi, J Med Internet Res 2010 April-June; 12(2); e14.
• US Dept. of Health and Human Services: Health Information Privacy: Research
  ▫ http://www.hhs.gov/ocr/privacy/hipaa/understanding/coverедentities/research.html