CS573 Data Privacy and Security

Data Privacy and Security in Healthcare

Li Xiong
Healthcare security and privacy

• HIPAA overview
• Research survey on information security and privacy in healthcare
HIPAA

• Health Insurance Portability and Accountability Act of 1996
• Title I – protects health insurance coverage
• Title II – regulates use and dissemination of health information
  – Privacy rule (effective in 2001, compliance date 2003)
  – Transactions and Code Sets Rule
  – Security rule
  – Unique identifiers Rule
  – Enforcement Rule
HIPAA Privacy Rule

• Privacy rule regulates the use and disclosure of Protected Health Information (PHI) held by “covered entities”
TO WHOM DOES HIPAA APPLY?

- Health Plans, including health insurance companies, HMOs, company health plans, and certain government programs that pay for health care, such as Medicare and Medicaid.

- Most Health Care Providers - those that conduct certain business electronically, such as electronically billing your health insurance including most doctors, clinics, hospitals, psychologists, chiropractors, nursing homes, pharmacies, and dentists.

- Health Care Clearinghouses - entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.
WHAT INFORMATION IS PROTECTED?

• HIPAA Regulates “Protected Health Information” (“PHI”)

• PHI is: information, oral or recorded, in any form or medium, that:
  – Is created or received by a provider, plan, etc.; and
  – Relates to past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or past, present or future payment for the provision of health care
WHAT IS THE SECURITY RULE?

• Applies to physical, technical and administrative requirements to protect maintenance, availability and confidentiality of PHI
• Closely intertwined with Privacy Rule
• Requires appropriate technological measures and physical security safeguards to maintain the security of PHI
• Will require Policies and Procedures and training for:
  – Password Maintenance
  – Access Controls
  – Physical Controls
    ➢ Logging off computers
    ➢ Screensavers
    ➢ Locking doors and files cabinets
  – E-Mail Risks
  – Other
WHAT IS THE PRIVACY RULE?

• A Covered Entity may only use or disclose PHI in certain circumstances

• Covered Entity must make reasonable efforts to limit use or disclosure of PHI to the “minimum necessary” amount to accomplish the intended purpose of the use or disclosure of the PHI
Principle of Disclosure

• The Privacy Rule establishes a list of acceptable and unacceptable ways to use PHI.

• The Privacy Rule may be waived by a signature of a patient.
  – Q: How many things do you sign when you go to the doctor?
  – Q: Do you know what they say?
Principle of Disclosure

• The Privacy Rule does, however, ensure that individuals have access to the information stored about them.
  – Also allows HHS to view your medical records when they’re “undertaking a compliance investigation”
De-identified Health Information

• No restrictions on the use or disclosure of de-identified health information

• A de-identification is achieved
  – by a formal determination by a qualified statistician or
  – Removal of certain identifiers (i.e., safe harbor rule.)
Explicitly Acceptable Disclosures

• Disclosure to the individual (required)
• Disclosure to: (allowed without consent)
  – Treatment Operations
  – Payment Operations
  – Health Care Operations
Explicitly Acceptable Disclosures

• Disclosure in Public Interest and Benefit Activities
  – Public Health (prevention or containment of a disease)
  – Employees where transmission of a dangerous disease was likely
  – Victims of abuse, neglect, violence, etc
  – Heath oversight activates and judicial proceedings
Explicitly Acceptable Disclosures

- Disclosure in Public Interest and Benefit Activities (cont’d)
  - Law enforcement purposes
  - Decedents
  - Organ, eye, tissue donations
  - Research purposes
  - Serious threat to public safety
  - ... and more...
Limited Data Set

• A limited data set is PHI from which certain identifier information is removed.
• Limited data set can be used for research purposes provided that the recipient of the data signs an agreement.
Authorized Uses and Disclosures

• All other uses and disclosures of data must have explicit written authorization by the individual.
Minimum Necessary Clause

• One of the central aspects of the entire Privacy Rule is that only the minimally necessary amount of PHI is disclosed.
• The minimum necessary clause does not cover:
  – Health care providers for treatment
  – Individuals who is the subject of the information
  – Disclosures made pursuant to an authorization
  – Disclosure to HHS or required by law
  – Disclosure for HIPAA compliance reviews
What does it mean to patients?
Right to Access

• Patients have the right to
  – Access or inspect their health record
  – Obtain a copy from their healthcare provider
    ➢ Reasonable fees may be charged for copying
  – Access and copying for as long as information is retained
  – There are a few exceptions
Doctor, I would like to see my medical records in regard to the period when my systolic ejection murmur was heard at the 2nd right intercostal space.

I'm sorry sir, but I never show my patients their records because they lack the knowledge needed to properly interpret the information.
Right to Amend

- Patients have the right to request an amendment (clarification or challenge) to their medical record
  - May need to put request in writing
  - Organization will review and determine if they agree or disagree
  - Request for amendment becomes part of permanent record.
Right to Account for Disclosures

• Patients have the right to request a list of when and where their confidential information was released
  – A list of disclosures (releases) within past six years (starting in April 2003)
    ➢ Date of disclosure
    ➢ Name of person or entity who received information and address if known
    ➢ Brief description of reason for disclosure
  – Exceptions: treatment, payment healthcare operations
Right to Request Restrictions

• The patient has the right to request an organization to restrict the use and disclosure (release) of their confidential information
  – Can request restriction in use of information for treatment, payment, or healthcare operation purposes
  – Organization is not required to agree with restriction(s)

• Patient can request to receive communication by alternative means or locations.
Right to File a Complaint

• The patient has the right to file a complaint if he or she believes privacy rights were violated*
  – Individual within the organization
  – The Secretary of the Department of Health and Human Services

*Organization must provide contact information for filing a complaint
Right to Receive Notice

• The patient has the right to receive a notice of privacy practices
  – Notice describes
    • How medical information is used and disclosed by an organization
    • How to access and obtain a copy of their medical records
    • A summary of patient rights under HIPAA
    • How to file a complaint, and contact information for filing a complaint
There Are Penalties

• Both criminal and civil penalties for:
  – Failure to comply with HIPAA requirements
  – Knowingly or wrongfully disclosing or receiving individually identifiable health information
  – Obtaining information with intent to:
    – Sell or transfer it
    – Use it for commercial advantage
    – Use it for personal gain
    – Use it for malicious harm
Penalties

• HHS may impose monetary civil penalties for violations of the Privacy Rule:
  – $100 per failure to comply with a Privacy Rule requirement (up to $25,000/yr/company for violations of the same Privacy Rule requirement)
Penalties

• Criminal Penalties
  – Any person (a physical person or an incorporated company) who knowingly obtains or discloses PHI is in violation of HIPAA and faces:
    • Up to a $50,000 fine
    • Up to a one-year prison term
  – An intention to sell, transfer, or use PHI increase both the fine and the prison term
Complaints related to HIPAA
Enforcement Results

Enforcement Results
January 1, 2007 through December 31, 2007

Total Resolutions 7,176

- Resolved After Intake & Review: 4,977 (69%)
- No Violation: 715 (10%)
- Corrective Action Obtained: 1,484 (21%)

Total Investigations 2,199

- Corrective Action Obtained: 715 (67%)
- No Violation: 715 (33%)
Legislative & Regulatory Needs

1. “Fixes” – problems that need to be addressed
2. “Challenges” – issues that need to be addressed, but for which we lack clarity about how to do so while minimizing cost and disruptions in health system operations
3. “Conundrums” – questions without obvious answers; need for further study
“Fixes”

• HIPAA Applicability Scope Tied to Administrative Transactions
  – Other provider organizations that do not participate in administrative transactions are not required to comply with HIPAA Privacy and Security Rules
  – Need to address all organizations that collect, receive, maintain, or use individually identifiable health information

• Inconsistent Applicability of Privacy and Security Rules
  – Privacy Rule applies to all individually identifiable health information
  – Security Rule applies only to electronic health information
  – Both need to apply to all identifiable health information, with appropriate provisions for electronic and non-electronic media
“Challenges”

• Notification of “Security Breaches”
  – Lack definition
  – Public notification may encourage others to exploit vulnerabilities
  – How to measure severity, intention, potential harm

• Right to Anonymous Care

• Accounting for Disclosures
  – Consumer has right to know who has accessed his or her health information

• “Healthcare Operations” Scope
  – Health information may be released without patient’s consent for purposes of treatment, payment, and “healthcare operations”
  – Need to constrain definition of “healthcare operations”
“Conundrums”

- Determining “Minimum Necessary”
  - Need to allow for context specificity

- “De-identification” of Health Information
  - Consumers with less common conditions, and consumers in sparsely populated areas are at higher risk of re-identification
  - Moving target – as systems become faster and more interconnected, “de-identification” becomes less feasible
  - In some cases, the ability to “re-link” health information to an individual is beneficial to the health and safety of that individual

- Sale of Health Information
  - Who owns the information – and therefore stands to profit from its sale?
  - Is ownership permanently bound with the individual about whom the information originally was collected? In other words, can ownership change once information is “de-identified?”
  - Is an individual’s authorization required in order to sell his or her health information?
Healthcare security and privacy

- HIPAA overview
- Research survey on information security and privacy in healthcare
Information Privacy and Security in Healthcare

Healthcare Consumers
- Personal Health Record Management
- Clinical Trial Participation
- Personal Disposition to Data Disclosure

Public Policy
- Medical Research
- Law Enforcement
- NHIN / RHIO
- Social welfare programs
- Disaster Response/ Disease Control
- Pricing of Health Services

Information Security
Threats to Information Privacy & Security [QL]

Providers
- Impact of IT on medical errors
- RFID deployment in medication admin.
- Risk analysis and assessment
- Telemedicine / eHealth
- Pervasive Computing in healthcare
- Operations management

Inter-Organizational
- Health Services Subcontracting
- Integrated Healthcare Systems
- Billing & Payment Efficacy

Inter-Organizational
- Access Control, [D]
- Data Interoperability, [D]
- Fraud Control [QN], [QL]
- Multi-institutional Network Security [D]

[D]: Design Research; [QL]: Qualitative Research ; [QN]: Quantitative Research
Privacy concern among healthcare consumers

• Use of identifiable information (Sankar et al., 2003)
  – Patients strongly believe that their information should be shared only with people involved in their care
  – Patients identify the need of information sharing among physicians
  – Many patients reject the notion of releasing information to third parties
  – Majority of patients believe they bear the responsibility of revealing genetic test results to other at-risk family members
Privacy concern among healthcare consumers

• Use of identifiable information (England, Campbell et al. 2007)
  – 28-35% of patients are neutral to their health information being used by physicians for other purpose
  – 5-21% of patients expected consent
Privacy concern among healthcare consumers

• Use/sharing of anonymized health records?
  – Very limited research
Privacy concern among healthcare consumers

• Disclose health information to online health websites (Bansal et al. 2007)
  – Current health status, personality traits, culture, prior experience with websites and online privacy invasions play a major role
Privacy concern among healthcare consumers

• Perceptions towards different types of personal health record systems
  – Relative perception of privacy and security concern increased with level of technology
    • Paper-based
    • Personal-computer based
    • Memory devices
    • Portal and networked PHR
Provider’s perspective

• HIPAA compliance behavior (Baumer et al. 2000)
  – Healthcare professionals were highly concerned about maintaining accuracy of patient records and about unauthorized access to patient data
  – Patient data should not be used for unrelated purposes except for medical research
Provider’s perspective

• Effect of HIPAA on medical research
  – Obtain consent from patients
  – Approval from IRB

• Researchers’ perspective (Ness 2007)
  – 68% of researchers felt HIPAA made medical research highly difficult
  – 25% believed that it has increased patients’ confidentiality or privacy
Provider’s perspective

• Effect of HIPAA on adoption rates of EMR (Miller and Tucker 2009)
  – hospitals in states with privacy laws were 24% less likely to adopt an EMR system
Access Control

• Role-based access control (RBAC) is generally presented as an effective tool to manage data access (Gallagher et al. 2002)

• Primary research
  – Algorithms to facilitate role-based access control
  – Contextual access control
  – Consent models to allow patients to define which component of a medical record can be shared and with whom
Access Control

• Healthcare organizations often adopt ‘Break the Glass’ (BTG) policies to facilitate timely and effective care

• Operationalisation remains a challenge (Rostad and Edsburg 2006)
  • 99% of doctors were given overriding privileges while only 52% required
  • Security mechanisms were overridden to access 54% of patient records
Access Control

• Research
  – Infer and construct privacy/security rules based on access logs from the actual workflow (Bhatti and Grandison 2007)
  – Audit logs to determine security/privacy violations (Ferreira et al. 2006)
  – Comprehensive auditing from disparate sources while ensuring patient privacy (Malin and Airoldi 2007)
Security/privacy in E-Health

• Health bank, personal health record service (not a HIPAA covered entity)
  – Google Health (retired)
  – Microsoft Health Vault
    • Account access and control
    • Record access and control
    • Microsoft uses aggregate information and statistics
Security/Privacy in E-Health

• E-health networks
  – Federated identity management (Peyton et al. 2007)
    • Establish a ‘Circle of Trust’ (CoT) for cooperating enterprises (hospitals, pharmacies, labs, ...) to offer web-based services to patients
    • A designated ‘Identity Provider’ manages pseudonymous identities of patients for transactions among partners
Security risks in authorized data disclosure

• Risks in sharing data for medical research
  – Identity disclosure
  – Attribute disclosure

• Research
  – Data anonymization
  – Statistical inference control
Information integrity in healthcare

• Integrity may be compromised due to faulty system design of clinical decision support system (Sijs et al. 2006)
  – Excessive alerts may cause ‘alert fatigue’ leading clinicians to override alerts
    • E.g. if drug X is taken AND drug Y is taken, then alert
  – Systems with high override rates may result in increased level of adverse drug events
Information integrity in healthcare

• Quality and reliability of patient data
  – Information errors from Computerized Physician Order Entry (CPOE) systems and disconnects from other information systems
  – 39% of health information managers indicated that their organisations have not adopted adequate timeliness policies to correct errors (Lorence 2003)
  – Medical research using perturbed/anonymized data
Financial Risk

• Healthcare fraud compromises 10% of total health expenditure (Dixon, 2006)
  – Medical identity theft
  – Fraudulent care and drug charges
  – Sale of medical identities to illegal immigrants
  – Fraudulent billing for services never received (also lead to erroneous health records)
Regulatory implications for healthcare practice

- Regulatory compliance issues from the providers’ perspective and other players such as employers, medical researchers, insurance
- Macroeconomic studies are needed to measure the effect of these regulations
Oh cool, they'll pay a fortune for this ... heyyyy, hang on ... who says I have anti-social personality disorder!
“Somehow your medical records got faxed to a complete stranger. He has no idea what’s wrong with you either.”
“Mrs. Cranley! You need to sign this HIPAA privacy form before the doctor can look at those warts on your stomach!”