



# **Privacy for Electronic Health Records: Legislative Compliance and Adequate Privacy Protection**

Tyrone Grandison, PhD  
Manager, Data Disclosure Research, Healthcare Informatics  
IBM Almaden Research Center  
[tyroneg@us.ibm.com](mailto:tyroneg@us.ibm.com)

# The Team

## ➤ People:

- Present: Karen Brannon, Sangeeta Doraiswamy, Stefan Edlund, Alexandre Evfimievski, Tyrone Grandison, Joshua Hui, Jerry Kiernan, Kun Liu, Karin Murthy, Evimaria Terzi Extended: Deon Glajchen, Christine Robson Past: Rakesh Agrawal, Dmitri Asonov, Roberto Bayardo, Alvin Cheung, Christopher Johnson, Ralf Rantza, Stefan Schönauer, Ramakrishnan Srikant, Raja Velu, Steve Watts, Yirong Xu

## ➤ Work:

- Created association rules - the basic building block for the field of data mining.
- Created the field of privacy-preserving data mining.
- Created Hippocratic Database technology – database that automatically protects the privacy of the information it contains.
- Created Theseos technology – middleware that enables privacy-preserving querying of a sovereign set of distributed RFID databases.
- Created Compliance Auditing technology - low-impact, efficient verification of policy.
- Created Sovereign Information Sharing technology – privacy-preserving sharing of information between sovereign entities without a third party.
- Created Database Watermarking technology – enables assertion of ownership over released or outsourced data. ....



# Agenda

- **Motivation**
- **What does Legislation Require: HIPAA Basics**
  - Covered Entities Under HIPAA
  - Summary of HIPAA Technical Requirements
  - Key Principles of the Privacy Rule (repeated for emphasis)
- **Evaluating Compliance versus Privacy Protection Required**
  - The Study
  - Evaluation
  - Insight
- **Desirable Technical Features of EHRs**
- **Conclusion**



# Motivation

- Privacy concerns are the main inhibitors to use and deployment of electronic health records
  - Concerns have begun to emerge at national level\*
  - Concerns about loss of reputation resulting from privacy breaches translating into increased spending on healthcare privacy compliance
  - In US, HIPAA is assumed to provide baseline for healthcare privacy protection.
- Led us to the question: **Does being compliant with regulation and law equate to protection for the patient?**
- Why is this question important? If the answer is negative then:
  - It puts the patient at risk
    - Results in false sense of privacy, i.e. purported compliance with privacy regulations
    - Undermines the notion of empowering the patient, i.e. Consent to a policy not a genuine reflection of privacy practices
  - It makes the existence of a policy insignificant
    - A policy does not reveal a company's true stance on data protection

\*Robert Pear. Warnings over Privacy of US Health Network. New York Times, February 18, 2007.



## Covered Entities Under HIPAA

### ➤ Covered Entities

- Include health plans, healthcare providers and healthcare clearinghouses
- **Health care clearinghouse** means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and “value-added” networks and switches, that does either of the following functions:
  - (1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.
  - (2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.” (45 CFR §160.103)
  - **HHS Comment** - “We note here that the term health care clearinghouse may have other meanings and connotations in other contexts, but the regulation defines it specifically, and an entity is considered a health care clearinghouse only to the extent that it meets the criteria in this definition.”

### ➤ Business Associate

- Performs functions or activities on behalf of, or services to, a covered entity involving the use or disclosure of PHI. (45 CFR §160.103)



# HIPAA Technical Requirements

## ➤ Access Controls – Security Rule

- Technical policies and procedures that allow access to only persons and software programs that have been granted access rights (45 C.F.R. §164.312(a)(1))
- Unique user identification – assign unique name or number for identifying and tracking user identities (§164.312(a)(2)(i))
- Emergency access procedure – ability to access PHI (§164.312(a)(2)(ii))
- Automatic logoff (A) – after period of inactivity (§164.312(a)(2)(iii))
- Encryption and decryption (A) – protection of stored PHI (§164.312(a)(2)(iv))

## ➤ Authentication

- Policies and procedures to verify that the person or entity seeking access to EPHI is the one claimed. (§164.312(d))

# HIPAA Technical Requirements

## ➤ Access/Disclosure Controls – Privacy Rule

- Policies and procedures designed to comply with Privacy Rule (§164.530(i))
  - Disclosure of PHI must be permitted or required by Privacy Rule (§164.502(b))
  - Limit internal access and use of PHI based upon role, purpose, conditions (§164.514(d)(2))
  - Limit disclosure of PHI based upon recipient, purpose, patient choices (§164.501 *et seq.*)
- Document policies and procedures in written or electronic format (§164.530(j))
- Minimum necessary disclosure (§164.502(b))
  - Make reasonable efforts to use, disclose, and request only the minimum amount of PHI needed to accomplish the intended purpose of the use, disclosure, or request.
- Authorization for uses and disclosures (§164.508)
  - Written authorization (or electronic signature) required for disclosure that is not otherwise permitted or required by Privacy Rule.
- Requests for restriction (§164.522(a))
  - Must enforce agreements for restriction, except in case of emergency for treatment purposes.



# HIPAA Technical Requirements

## ➤ Audit Controls

- Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI. (§164.312(b))
- Disclosure auditing – covered entity must account for disclosures of PHI (with certain exceptions) for the past six years, but after compliance date. (§164.528)
- For each access or disclosure, must account for:
  - User identity, time, role, purpose, recipient, and patient authorization (if any), and
  - The actual information disclosed. (§164.528(b)(2))

## ➤ Integrity

- Electronic mechanism to authenticate EPHI – corroborate that it has not been altered or destroyed in an unauthorized manner. (§164.312(c)(2))



# HIPAA Technical Requirements

## ➤ Security in Transmission

- Security measures to assure that electronically transmitted EPHI is not improperly modified without detection until disposed of. (§164.312(e)(2)(i)).
- Data in transit over a network - Mechanism to encrypt electronic protected health information (in transmission) whenever deemed appropriate. (§164.312(e)(2)(ii))

## ➤ Individual Right of Access

- Provide access to patients to obtain designated record set. (§164.524)
- Does not have to be in electronic format.

## ➤ De-Identification

- Limited data set – may be used with data use agreement. (§164.514(e))
- De-Identified PHI – not subject to HIPAA restrictions. (§164.514(b))



## Key Principles of the Privacy Rule

- **Notification:** Patient should receive notice of covered entity's privacy practices.
- **Authorization and Consent:** Written authorization required for disclosures not permitted under Privacy Rule.
- **Limited Use and Disclosure:** Covered entities must ensure use and disclosure of *minimum necessary* PHI for a specific purpose.
- **Auditing and Accounting:** Patients have the right to accounting of all disclosures of their PHI.
- **Access:** Patients have the right to access their records maintained by the covered entity.



## The Study

- We picked the top 30 hospitals, as specified by the 2005 hospital data compiled by the American Hospital Association.
- We created a matrix of desirable properties for the Privacy Rule.
- We examined the HIPAA Notice of Privacy Practices (NOPP) and the Website Privacy Policies of these institutions and evaluated them against our ideal.



# Notification, Authorization and Consent

- Policies state that consent is implied by visiting the website
  - Not quite the best practice to meet the Notification requirement
  
- No policies are available in a form amenable to electronic manipulation.
  - Precludes automated interpretation and analysis for **informed consent**
  
- Policy updates communicated with little regard for patient
  - Insufficient to only post them on website
  - Patient consent to updated policy not obtained
  
- Compliant with HIPAA
  - HIPAA does not require policy to be posted using machine-readable format
  - HIPAA does not require policy to be communicated using expedient means (such as email, IM)



## Limited Use and Disclosure

- Policies define broad and all-encompassing purposes
  - E.g. “administering healthcare”
  - Subsumes a huge category of uses and disclosures
  
- No fine-grained list of employee categories or roles with authorizations to view specific categories of patient data
  - E.g. “members of medical staff” category includes most employees
  - Provides umbrella authorization for employees
  - Criterion for authorization or exception-based accesses (i.e. “break the glass” privileges) not specified. Exception mechanisms being increasingly utilized
  
- Compliant with HIPAA
  - HIPAA has provisions to let organizations design policies with broadly-defined purposes
    - E.g: While “Marketing” is a purpose requiring explicit authorization, a sub-category “communications for treatment of patient” is exempt and can be exploited
  - HIPAA calls for policies and procedures for controlling access to PHI but does not require stringent technical mechanisms to be in place



## Audit and Accounting

- Most organizations maintain audit trails for all actions pertaining to PHI to meet audit reporting and accounting requirement
  
- However, there is still much left to be desired
  - Audit logs in current systems do not capture all necessary contextual information (such as purpose or recipient)
  - Accounting for data disclosures is ineffective in improving levels of privacy protection unless shortcomings in disclosure policies are first addressed
    - E.g.: broadly-defined purposes, umbrella authorizations, exception-based accesses
  - While using audit as a deterrent factor, organizations should not fail to do better by providing more proactive protection



## Access

- All policies indicated that patients have a right to access their information through phone, email or online account
- Concerns:
  - Ability to access/update personal information provides no measure of how much information is actually protected unless patient is in control of his/her disclosure policy
  - The process of information access may be simple or laborious- from being a matter of few mouse clicks to a waiting period of up to 60 days; recent information disclosures may not get reported



## Insight from the Study

- Compliance with HIPAA in its strongest form may be a decent start to ensure adequate patient privacy protection.
- Industry practice is to aim for minimal compliance, which is not desirable from a patient standpoint. NOPPs and Website Privacy policies cover enough ground to enable regulatory compliance.
- Thus, currently compliance with law is not an accurate measure of the level of protection afforded to patients. Current policies and measures are inadequate to communicate understandable privacy practices or provide adequate privacy safeguards to the patients
- EHR technology need to aim for a higher standard.



# Desirable Technical Features for EHRs

## ➤ Access/Disclosure Controls

- Electronic patient authorizations and consents
- Support fine-grained policy modifications by patients
- Electronic patient designation of representatives
- Resolve conflicts among multiple policies

## ➤ Audit Controls

- Account for all past disclosures of PHI
- Allow patients to run their own disclosure audits
- Analyze circumstances of modifications to PHI and policies
- Provide meaningful summaries of audit results
- Trace lineage of information to assess data quality



# Desirable Technical Features for EHRs

## ➤ Information Leakage Controls

- Examples - watermarking, fingerprinting, query ranking

## ➤ Secure Audit Logs

- Ensure that logs are resistant to tampering

## ➤ Individual Access

- Online patient access to designated record set
- Ability of patients to download and transfer EHR

## ➤ Lifecycle Management

- Define data retention policies
- Delete expired data without affecting ability to recover other data



## Conclusion

- Privacy is still an important concern for EHRs. Despite institutional push for compliance with privacy legislature, it is not a solved problem.
- The emphasis should move from one of compliance to one of patient protection in order to enable the EHR systems that can be trusted.



<http://www.almaden.ibm.com/cs/disciplines/iis/>