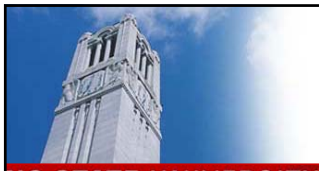


NC STATE UNIVERSITY Computer Science

Security & Privacy Requirements for Healthcare Applications

Guest Lecture for CSC 712

Qingfeng He

North Carolina State University

qhe2@eos.ncsu.edu

August 24, 2005

Methodology

HIPAA, Organizational Policies, Requirements Specifications

↓

Security and Privacy Goals

↓

Security and Privacy Requirements for the EMR project

↓

Security and Privacy Design

What is HIPAA

- In 1996, Congress enacted the Health Insurance Portability and Accountability Act (HIPAA), one purpose of which is to protect health information by establishing transaction standards for the exchange of health information, security standards, and privacy standards for the use and disclosure of individually identifiable health information. There are three main components:
  - Protection for the privacy of Protected Health Information
  - Protection for the security of Protected Health Information
  - Standardization of electronic data interchange in healthcare transactions

Protected Health Information (PHI)

- PHI is any health information that can be used to identify a patient and that relates to the patient, health care services provided to the patient, or the payment for these services.
- PHI includes
  - All medical records and other information that identifies the patient, including demographic, medical, financial information
  - The above information in any form—electronic, paper, or spoken

Understand Security and Privacy

- What are basic security goals?
- What is privacy?

Information Security

- The purpose of information security is to protect the confidentiality, integrity, and availability of information.
  - Confidentiality means that data or information is not made available or disclosed to unauthorized persons or processes.
  - Integrity means that data or information has not been altered or destroyed in an unauthorized manner.
  - Availability means that data or information is accessible and useable upon demand by an authorized person.
- More security goals:
  - Accountability means the ability to identify who or what was responsible for taking a particular action.

What is Privacy?

- The right to be let alone [Warren & Brandeis 1890]
- Privacy is the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others [Westin 1967]

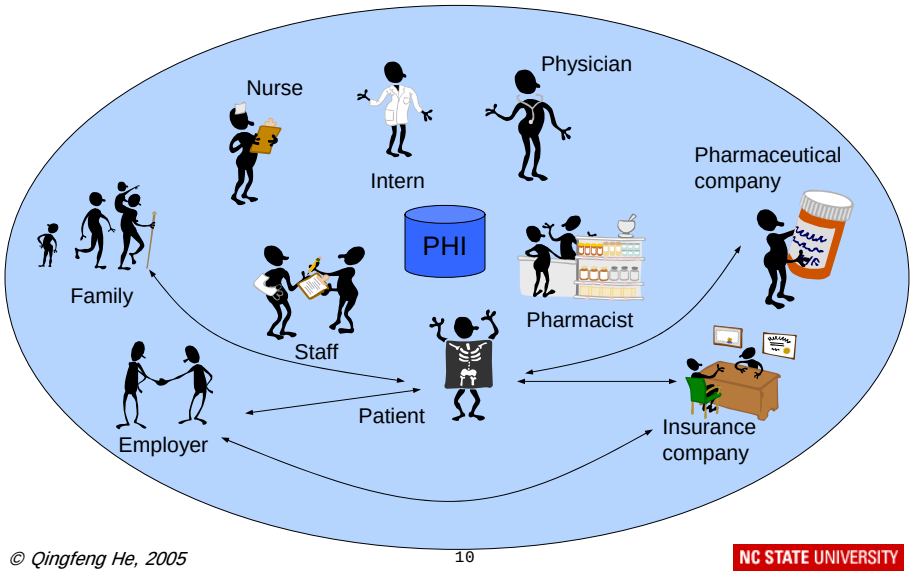
Privacy Principles

- Fair Information Practices (FIP) Principles
  - Notice/Awareness
  - Choice/Consent
  - Access/Participation
  - Security/Integrity
  - Enforcement/Redress
- OECD guidelines
  - Collection Limitation Principle
  - Data Quality Principle
  - Purpose Specification Principle
  - Use Limitation Principle
  - Security Safeguards Principle
  - Openness Principle
  - Individual Participation Principle
  - Accountability Principle

Information Privacy

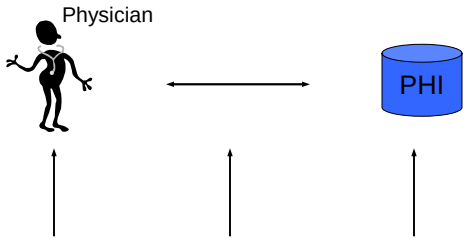
- Privacy means that data is used only for authorized purposes, based on legal requirements, organizational policies and end-user choices.
  - Data subject participation
  - Data subject consent
  - Data subject choices
  - Data subject control
  - (Purpose binding)
  - (Minimum data collection)

The Electronic Medical Records (EMR) Project



Confidentiality & Integrity

- How can we elicit the requirements to achieve confidentiality & integrity for the EMR project?



(1) User Side

- User identification/authentication
- Example requirement:
  - The system shall authenticate every user before he/she can access any information in the system.
  - Details:
    - ✓ Password requirements: Length? Special characters? Must change every 3 months? Password retrieval/reset?
    - ✓ Username requirements: Special characters? Can a user change his/her username?
    - ✓ Other authentication methods: biometric?

(2) Communication Channel

- Example requirement:
  - All data transferred over a networking channel shall be encrypted.
  - Details:
    - ✓ Standard SSL?
    - ✓ 128/256 bits encryption?

(3) Server / DB Side

- Data Authentication:
  - Message Authentication Code (MAC)
  - Digital signature
- Secure data storage
  - What data shall be encrypted before stored in the system?
    - ✓ Passwords, SSN, other extremely sensitive information
- Authorization
  - Access control (most challenging part)
  - The HIPAA security regulation Section 142.308(c)(1)(i)(B) requires the use of either
    - ✓ Role-based Access Control
    - ✓ User-based Access Control
    - ✓ Context-based Access Control
- Accountability
  - Auditing trail

Privacy Requirements

- Data subject participation
  - Every data subject shall be able to update his/her personal information (e.g., contact information) to ensure accuracy.
- Data subject consent
  - Which kind of data access requires the consent from subject?
  - HIPAA prescribes that healthcare practitioners cannot use or share PHI unless:
    - ✓ authorized by the patient, or
    - ✓ required or authorized by law to use or share the information
- Data subject choices
  - Allow data subject to opt-in/opt-out from certain services

Privacy Requirements (Cont'd)

- Data subject control: every data subject can specify who can access what information
- Main part of the EMR project?
- The process is called access control policy specification [He05]
  - <mode, subject, action, object, condition, obligation>

ACP Specification Process

- Identify and classify information
- Identify users of the system
- Identify users' interactions with the system
- Define conditions and obligations for the ACP

Identify and Classify Information

- Identify information that is stored in the system
- Classify them according to sensitivity
  - Extra private
  - Private
  - ...
- Determine the general access principle for each kind of information
- Process and organize information, if necessary
  - For example, de-identify information

De-identified Information

- The following identifiers of the individual and the individual's relatives, employers, and household members all must be absent from the PHI to designate it as "De-identified".
  - 1. Names;
  - 2. All geographical subdivisions smaller than a State;
  - 3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission/discharge dates, date of death; and for persons over eighty-nine years of age all dates including year;
  - 4. Telephone numbers;
  - 5. Fax numbers;
  - 6. Electronic mail addresses;
  - 7. Medical record numbers;
  - 8. Health plan beneficiary numbers;
  - 9. Account numbers;
  - 10. Certificate/license numbers;

De-identified Information (Cont'd)

- 11. Vehicle identifiers & serial numbers & license plates;
- 12. Device identifiers and serial numbers;
- 13. Web Universal Resource Locaters (URLS);
- 14. Internet Protocol (IP) address numbers;
- 15. Biometrical identifiers, including finger and voice prints;
- 16. Full face photographic images and any comparable images;
- 17. Any other unique identifying number, characteristic, or code except for secure reidentification or data matching codes that are not derived from information about the individual.

Identify Users of the System

- Classify users according to their role
  - Physician
  - Surgeon
  - Nurse
  - Resident
  - Pharmacist
  - ...
- Role hierarchy may be defined, if necessary
  - Every sub-role inherits all privileges of its super-role

Identify Users' Interactions with the System

- Use Cases
- Scenarios: a sequence of events in normal, iterative, alternative flow
  - Events: actor, action, object
  - Pre-conditions/post-conditions
  - Requirements
  - Goals
  - Obstacles
  - Sources

Example Scenario

- [**Goal**] Register patient into the EMR system
- [**Domain**] EMR Patient Information Management
- [**Scenario**] Ward secretary registers patient into the EMR system
- [**Actors**] Ward secretary
- System
- [**Events**] Ward secretary invokes patient registration procedure
- Alt Branch 1: System already stores the patient's info
- Ward retrieves patient's info based on patient # or name
- …
- Alt Branch 2: System does not have the patient's info
- Ward secretary create a new record for the patient
- System saves PHI and shows confirmation
- System generates auditing trail
- [**Preconditions**] Ward secretary authenticated
- Ward secretary trained in privacy and security
  Hospital security and privacy training process documented
- [**Postconditions**] Registration audit trail generated
  Patient registered in the EMR system

Define Conditions and Obligations for Each Access Control Policy

- Very challenging to define complete conditions
- Some thoughts to help ensure better coverage:
  - Data subject's predefined rules
  - System-wide rules
    - ✓ For example, global access rules for extra-private information
  - Common kinds of constraints [He05, Table B.4 on page 185]
    - ✓ Authentication constraints
    - ✓ Contextual constraints (Temporal, Location, Relationship, Affiliation, Attribute, State)
    - ✓ Usage constraints
    - ✓ Database constraints
    - ✓ Security constraints
    - ✓ Privacy constraints

References

- [He05] Q. He. Requirements-based Access Control Analysis and Policy Specification. *PhD Dissertation*, North Carolina State University, Raleigh, NC, 2005.

An electronic version is available at NCSU library.