Toward segmentation

"Getting IT Right: Protecting Patient Privacy Rights in a Wired World”

Lee Tien <tien@eff.org>

Electronic Frontier Foundation

June 13, 2011

Health IT system goals?

- Stores patient records with data from multiple sources
- Provides differentiated data access to doctors/others based on role, need, specialty, etc.
- Protects patient data at granular level
  - users don't necessarily get access to entire record – e.g., sensitive information more highly protected

Such systems exist

- Currently operating in a variety of information environments that handle large data sets
- Permissions systems have been built to model multi-level classification systems used by defense, intelligence, and law enforcement
  - E.g. Palantir Technologies, www.palantirtech.com
- Can we adapt such permissions systems for health IT?

Challenge 1: coherent system

- Two main requirements
  - Clear, dynamic schema that accurately models universe of health information
  - Ability to pull information from various sources while avoiding unnecessary centralization of data

Traditional DB model

- Most DBs treat record as single row

Patient	Date of Office Visit	Procedure A Test Result
Joe	12/1/10	Negative

- This model becomes unwieldy and slow

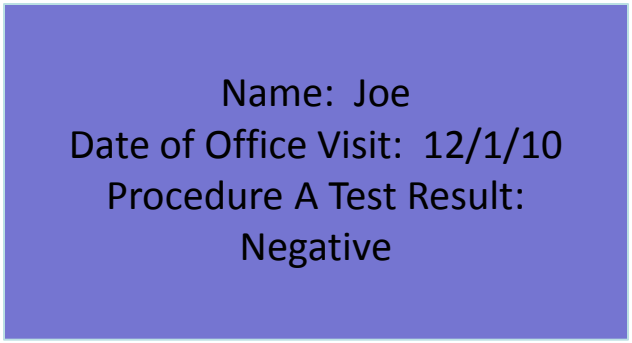
Patient	Date of Office Visit 1	Date of Office Visit 2	Date of Office Visit 3	Procedure A Test Result	Procedure B Test Result	Procedure C Test Result
Joe	12/1/10	12/3/10	12/14/10	Negative	Negative	
Jane	12/4/10	12/7/10			Positive	Negative

Object model

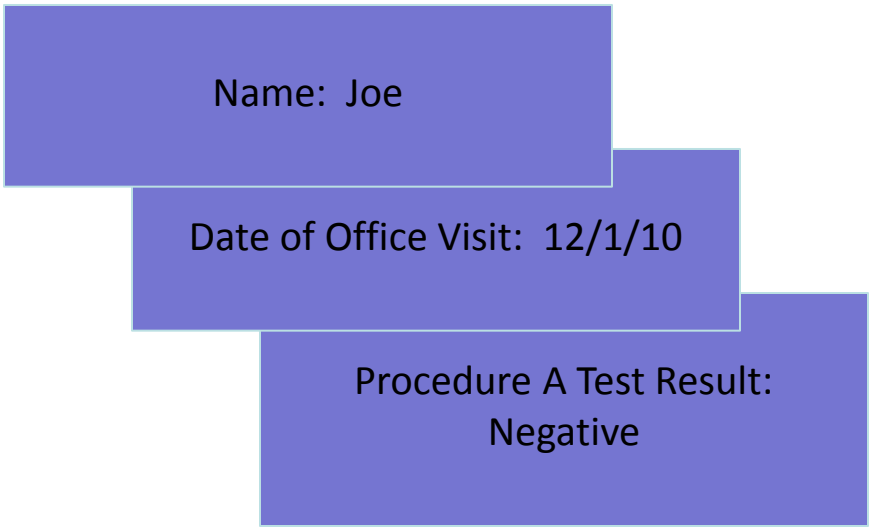
- Think of DB as stack of cards
- Each “card” contains single data point
- Complete patient record created by compiling cards together

Comparison

- Traditional model best thought of as a single card:



- Object model more like stack of cards



Challenge 2: privacy controls

- Different actors have different needs when accessing patient records
- Most system users don’t need to see entire patient record to perform task
- Can construct IT system that protects on a data-point-by-data-point basis — not record-by-record

Weakness of traditional model

- Access controls protect data on row-by-row basis

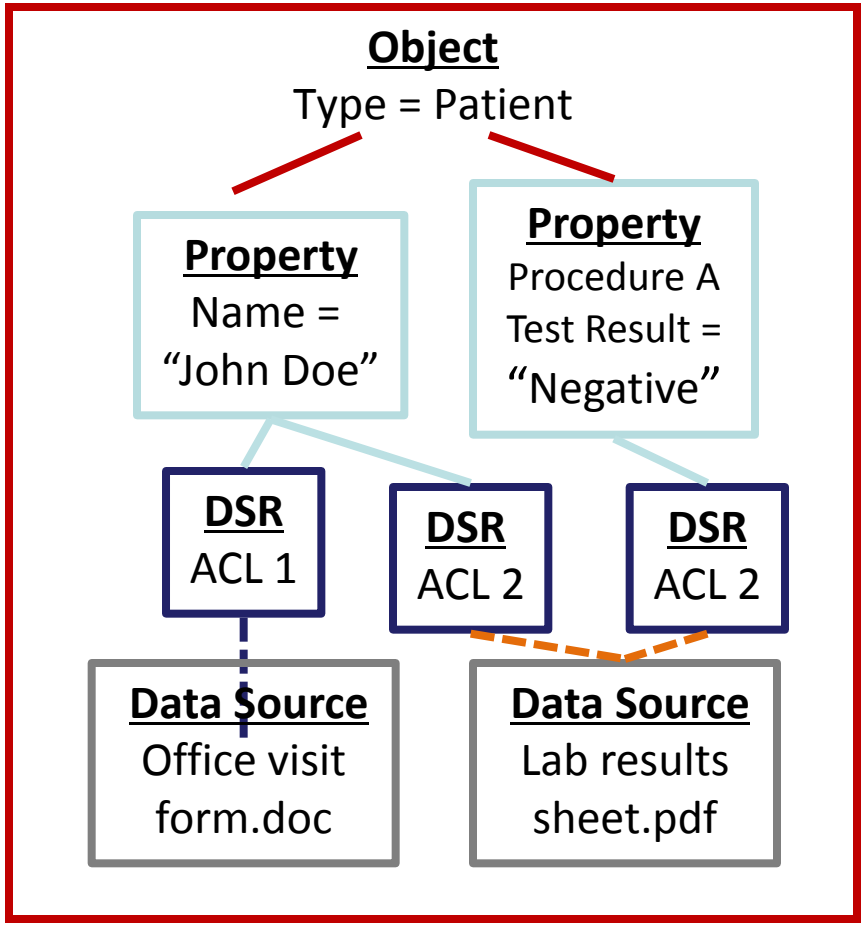
Patient	Date of Office Visit 1	Date of Office Visit 2	Date of Office Visit 3	Procedure A Test Result	Procedure B Test Result	Procedure C Test Result
Joe	12/1/10	12/3/10	12/14/10	Negative	Negative	
Jane	12/4/10	12/7/10			Positive	Negative

- Allows user to see all data about Joe, even if only data relevant to task is name, specific test result

Object DB conceptual view

Each data point in a record is linked to a source document via data source record (DSR)

- DSR contains Access Control List (ACL) of authorized users
- ACL derived from access controls applied to source document by original data owner



Access control

- Each ACL group can have one of four permissions governing how users in that group can interact with the data:
  - **Discovery** – User is told additional data exists in a record but must contact the data owner to see it
  - **Read** – User can see a data point
  - **Write** – User can see and edit a data point
  - **Ownership** – User can see, edit, and set access controls on a data point

Example

- Joe's medical record is as follows:
  - Name: Joe
  - Office visits (with related notes):
    - 12/1/10
    - 12/3/10
    - 12/14/10
  - Procedure A Test Result: Negative
  - Procedure B Test Result: Negative
  - Procedure C Test Result: Positive
- Joe's positive test result results in his being referred to a specialist. Dr. X shares his medical records with the specialist, Dr. Y.
- Notes on Joe's first two office visits and the results of Procedures A and B are irrelevant to the specialist
- How would the record be shared under this system design?

Setting up the ACLs

- ACL Group 1: Dr. X, Permissions - Ownership
- ACL Group 2: Dr. Y, Permissions - Read
  - Name: Joe (ACL 1), (ACL 2)
  - Office visits (with related notes):
    - 12/1/10 (ACL 1)
    - 12/3/10 (ACL 1)
    - 12/14/10 (ACL 1), (ACL 2)
  - Procedure A Test Result: Negative (ACL 1)
  - Procedure B Test Result: Negative (ACL 1)
  - Procedure C Test Result: Positive (ACL 1), (ACL 2)

Result

- Dr X sees:
  - Name: Joe
  - Office visits (with related notes):
    - 12/1/10
    - 12/3/10
    - 12/14/10
  - Procedure A Test Result: Negative
  - Procedure B Test Result: Negative
  - Procedure C Test Result: Positive
- Dr Y sees:
  - Name: Joe
  - Office visits (with related notes):
    - 12/14/10
  - Procedure C Test Result: Positive

Challenge 3: accountability

- System must make users accountable
- All edits (additions, modifications, deletions) to records must be tracked to the user responsible
- The auditing must be done in real-time to allow for the quick identification of misuse
- The audit trail must be immutable to ensure the integrity of the data

“Revisioning database”

- This detailed record history can be accomplished using a “revisioning database”
  - every addition, edit or deletion results in a new line of information added to the record
  - these additions, edits, and deletions can be tracked to the individual who entered them
- Documents complete history of a record
- Combined with traditional audit logging capabilities, helps ensure that data stewards can detect either intentional or accidental misuse

Summary

- Granular meta-tagging DB technology exists and is in use today in high security information environments
- A health IT system can offer patients the same level of protection while also sharing information necessary to allow doctors and other users to do their jobs
- (but probably doesn’t solve inference attacks)