SITH2, Panel 4: Secure Audit
Joe Hall, New York University
May 16, 2012

1) Introduction

• Postdoc at NYU working under Helen Nissenbaum.
• SHARP-S grant, security & privacy
• We are part of the policy team
• Background in hard science, astrophysics, modeled planetary atmospheres in F77

2) Want to pull back and discuss policy

• What kinds of policy should exist around user-access to information about PHI disclosure? Audit data?
• Overview:
  A) What are the current and proposed policy mechanisms?
  B) What are the implications of user access to audit data?
  C) What are some useful directions?
    • Involving users in auditing.
    • More useful artifacts for disclosure/use monitoring

A) What mechanisms currently exist?

• The Privacy Rule is structured around Fair Information Practice Principles (FIPPs).
• One of those principles says that data subjects (patients) should be able to understand how PHI is disclosed.
• The privacy rule uses something called an “Accounting of Disclosure” (AOD).
  o Patients can request an AOD and Covered Entities have to provide a dossier that outlines how their PHI has been disclosed for 6 years.
  o Focuses on disclosures made outside the organization boundary
  o Subject to a number of exemptions...TPO, Law Enforcement
  o Includes: data, recipient, what was disclosed, purpose.
• HITECH changed this
  o It’s rare to see legislation directly modify a regulation!
  o HITECH removed the exemption for accounting for TPO – via EHRs!
  o Also shortened the time period from 6 to 3 years.
  o OCR at HHS issued a proposed rule to modify AODs
    ▪ Intended to make AODs easier in a number of ways.
    ▪ Two rights: an AOD, an Access report
    ▪ The access report would have provided a list of all accesses to PHI in an “electronic designated record set” over three years.
    ▪ Included internal accesses for TPO.
    ▪ Only applied to electronic records
    ▪ Would have established an inclusive rather than exclusive list.
• A number of problems:
  o eDRS is much, much more than EHR/EMR system!
  o Many of these systems do not have audit logs.
    ▪ Security Rule doesn’t technically require them! “Must make reasonable and appropriate audit methods” (can be real-time)
  o Patients don’t use the AOD now. Don’t understand them.
    ▪ 50% don’t ever receive requests, only 6% receive

B) What are some implications for user access to audit data?

• Proprietary concerns – expose quite a bit about operations
• Quite opaque artifact – patients may feel that something funny is happening, when they just don’t understand healthcare.
• Serious safety issues – domestic violence, child/adult abuse or neglect, dangers to the workforce (mental, criminal)
• Lack of understanding of public health and research uses.

C) What are some useful directions?

• It’s clear it could be very useful to involve patients in auditing.
• Institutions and patients don’t have aligned interests in monitoring PHI use/disclosure.
  o CEs want to avoid liability and improve processes.
Patients have many interests but in the end it is PHI about them and that’s an invested interest.

- Involving users in monitoring use/disclosure distributes the audit problem, so that it’s not a human doing statistical auditing or algorithms focusing on institutional interests.
- However, is an AOD or Access report the right thing?
  - Both are big stacks of line-by-line information
  - Access reports for a typical hospital stay, could be hundreds of pages long.
  - Completely lacking in contextual information!
  - We’ve started to think about what would be more useful to patients.
    - “What do they care about?”
    - “What surprises them?”
  - We have an initial proposal that we’re working on w/ Benedicte Callan of the University of Texas (public policy)
    - Idea is rather than disclose audit logs, why not aggregate audit logs across patients?
    - This would be an “Accounting of Relationships” (AOR) and would be sort of like an SEC filing that gave publicly available evidence of the information flows an institution participates in.
      - Would allow comparisons!
      - Also could be useful as a complement to AODs. Show only the flows your PHI participates in.
      - Still some problems (privacy, enforcement)