Context is King and Clarity is Prime Minister

Presented to: Redwood Mednet's Connecting California Conference 2011
By Laura Landry, Executive Director, laura.landry@whinit.org, 562-436-2923

Goals

- Set the Stage for ACTIONABLE privacy and security discussions in California and the U.S.
- Build momentum and consensus for forward movement
- Recruit participants to build out the rational roadmap and model(s)

Definitions

- ***Context***
  - 1. The circumstances that form the setting for an event, statement, or idea, and in terms of which it can be fully understood and assessed.
  - 2. The parts of something written or spoken that immediately precede and follow a word or passage and clarify its meaning.
- ***Privacy***
  - a : the quality or state of being apart from company or observation : seclusion b : freedom from unauthorized intrusion <one's right to privacy>
  - 2archaic : a place of seclusion
  - 3a : secrecy b : a private matter : secret

- Confidentiality
- **1:** marked by intimacy or willingness to confide <a *confidential* tone>
- **2:** private, secret <*confidential* information>
- **3:** entrusted with confidences <a *confidential* clerk>
- **4:** containing information whose unauthorized disclosure could be prejudicial to the national interest — compare secret, top secret

The Mythological Origins

- Privacy and Security
  - A California citizen has a "right to privacy"
    - Except when it is bargained away under contract for some reason
- The nation is in an uproar around consumer privacy
  - The average person assumes healthcare has what it needs to do their jobs
- Healthcare has played fast and loose with patient information
  - Sometimes intentially selling patient data for profit
  - Often just making mistakes with the best of intentions

The Furor

- It's a NUMBERS game
  - If someone loses a paper chart
    - It's one person's data
  - If someone loses a disc of data or is hacked
    - It's data in the thousands
  - And that data can be used to steal identities or commit fraud
- Do organizations need to be diligent? Yes!
- Have we jumped the shark? Yes!

Expectations of Privacy -- Demystified

Context	Financial Responsibility	Privacy Expectation	Expectation of Confidentiality
EmergencyRoom	3rd Party	Low	High
Encounter	3rd Party	Low	High
Encounter	Patient	High	High
Encounter	No Pay/Charity	Low	High

Further, Privacy from WHOM?

- Physicians? No
- Care team? No
- Employers? Yes
- Payers? Yes

- Do my privacy requirements change from time to time?
  - Yes

Higher Standard for Electronic Data

- See slide that says "thousands of records with identity information"
  - Current paper breaches are one at a time, or at worst hundreds at a time
- Banks manage to keep private records private
  - Healthcare delivery resources have varying levels of expertise
  - It is an unfunded mandate – nobody pays a "security transaction fee" to healthcare providers

So what are we all afraid of?

- Lawsuits
  - Deep pockets pay high fines
- No industry agreement on what works
  - Or even what needs protecting
- Nobody knows what "Enough" is

Protect the data – it's a reasonable request

- The HIT industry does not put a high emphasis on determining the requirements
- The HIT users do not put a high priority on having their vendors solve the problems
- At the most basic level, the way we think about protecting data is archaic, at best
- This isn't rocket science, we have industrial best practices from many places

So what's the Roadmap?

- Transparency
  - Why do people exchange data and for what purposes
  - Auditability – the patient should know the roles of people who have accessed their data
- Precision
  - The industry must agree to the scenarios, and use the right terms to describe the access to data
  - Impermissible uses must be clearly spelled out
- Working together to drive the HIT industry to develop "self-aware data" so that rules can be applied to it for a variety of circumstances