HIE privacy concerns

2011 Redwood MedNet Privacy and HIE workshop

Lee Tien tien@eff.org

Senior staff attorney

Electronic Frontier Foundation

My background

- Privacy law specialist/generalist
  - Focus: privacy/security of devices and networks
- 4th A, state constitution, PATRIOT Act, Wiretap Act, Stored Communications Act, Fair Information Practices….
- Current issue areas: communications and transaction surveillance, location tracking, biometrics, national ID/ID mgmt, “smart grid,” EHR privacy/security

General lessons

- When systems really go digital, huge changes for privacy and security
  - More data, bigger stores of data
  - Data moves faster to more places/people
  - More/faster/better data-mining/analysis
- Failures can be much worse
- Complex systems harder to design well

HIT systems are complex

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

“Best practices” concerns?

- Patient consent and informing
- “Minimum necessary”
- Segmentation (sensitive, patient choice)
- De-identification, re-identification
- Focus: *what “authorized” entities do with patient data*
- (not data breaches, trespassers, etc.)

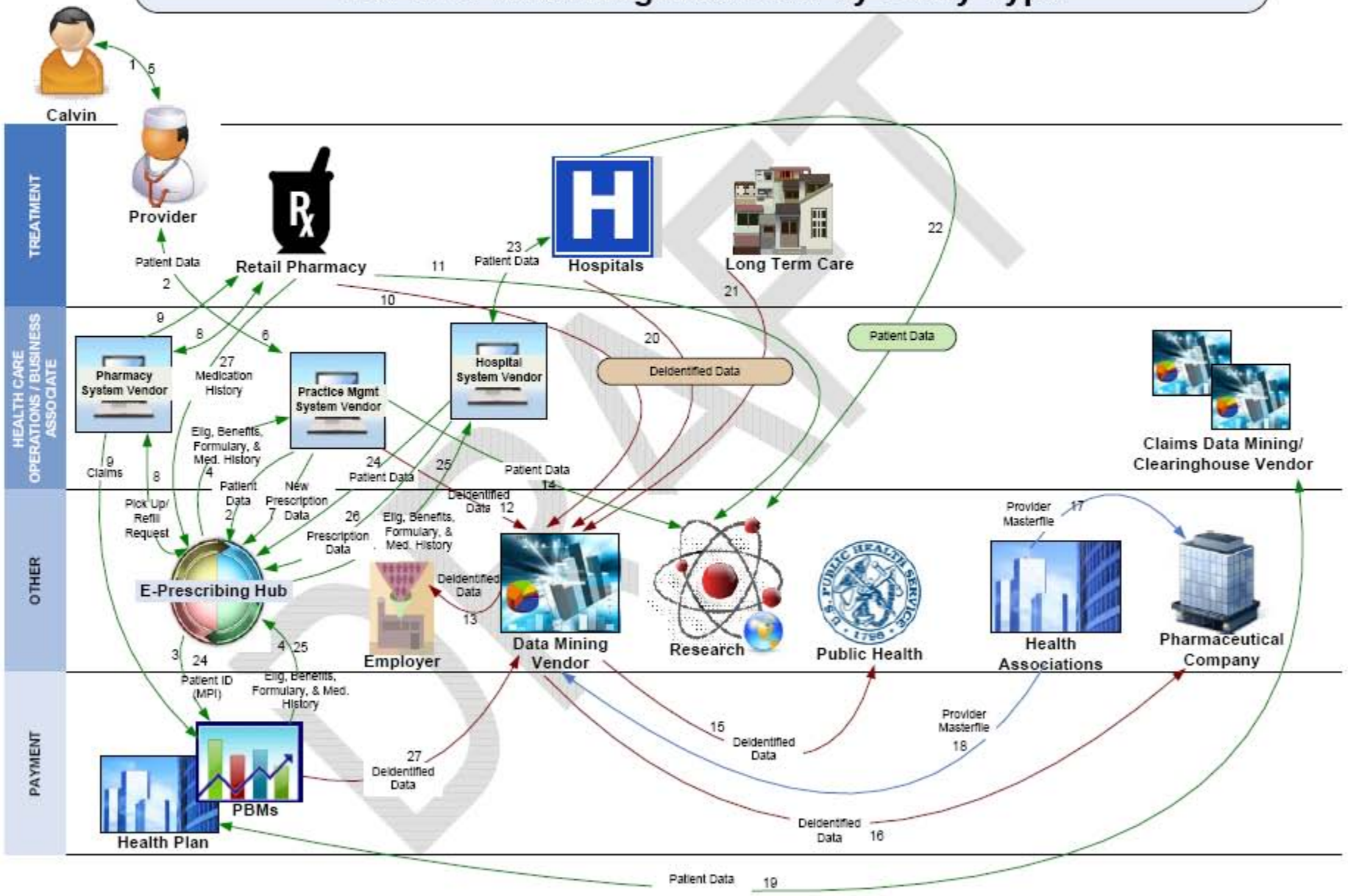
What's the right perspective?

- These issues mix technology and policy
- But more important, draw on deeply held social norms/values
- People believe in and want to believe in strong medical privacy, strong doctor-patient confidentiality

Privacy of patient data …

- … is necessary if patients are to trust the healthcare system is really about *their* care
- Increased electronic “sharing” or dissemination makes patients nervous

Use of ePrescribing Data Flow by Entity Type



2010 CHCF study

- 42% uncomfortable with EHR sharing even if name, DOB, address, and SSN would not be shared
  - Another 25% unsure
- 15% said they'd hide information from their doctor
  - Another 33% would consider it

Challenge 1: data flow candor

- People generally don't know who gets their data, why, how, etc.
- It will get worse, so how do we make sure patients aren't surprised?
  - Especially important for sensitive health information
  - But also sensitive recipients, e.g. employers

Perverse incentives

- Economic/commercial incentives for non-treatment uses of patient data
  - EFF criticized PCAST emphasis on exchange to promote innovation and entrepreneurship; placing these goals on a par with patient care risks the privacy and security needed for patient trust
- Research, public health raise like issues
- Social control incentives?

Challenge 2: accountability

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