Data Breach Lessons from the Trenches: A Retrospective and Forecast

Rick Kam
President and Co-Founder
ID Experts
February 6, 2014

HIPAA Summit 2014. Washington, D.C.
Retrospective

• Move to electronic health records
• Increased legal and regulatory risk
• Health information and insurance market exchanges
Retrospective

- Omnibus Rule Implications
  - HITECH privacy/security now applies directly to business associates
  - CEs and BAs need to embrace new definition of “breach”
  - “Ownership” of data becomes more fluid
Retrospective

- Convergence of Risk
  - Mobile, Cloud, BYOD
  - “Black market” value of PHI/PII
  - Increased reputational, medical, and other risks from loss and/or other unauthorized disclosure of PHI
Patient Privacy & Data Security Study

Experienced a data breach involving the loss of patient data in the past two years.
Patient Privacy & Data Breach Study

Type of data that was lost or stolen

- Medical file: 48% (FY 2012) vs. 47% (FY 2011)
- Insurance record: 48% vs. 49%
- Payment details: 24% vs. 17%
- Prescription: 20% vs. 19%
- Schedule: 19% vs. 25%
- Stim: 15% vs. 20%
- Other: 2% vs. 3%
Patient Privacy & Data Breach Study

Type of device compromised or stolen

- Desktop or laptop: FY 2012 - 38%, FY 2011 - 43%
- Smartphone: FY 2012 - 24%, FY 2011 - 21%
- Tablet: FY 2012 - 15%, FY 2011 - 7%
- USB drive: FY 2012 - 13%, FY 2011 - 16%
- Server: FY 2012 - 5%, FY 2011 - 7%
- Notebook: FY 2012 - 2%, FY 2011 - 4%
Summary of Trends

- More data privacy incidents
- More PHI data loss (i.e. health insurance info)
- Increased risk from tablets
Lessons from the Trenches

• If you don’t have a documented security risk analysis, including actions you’ve taken to address risks, you are exposed, no matter your size

• It is a “brave new world” for HIPAA business associates; get ready

• Organizations are evolving governance models for privacy & security; some trend towards unifying these responsibilities and report structure to board

• Need to “operationalize” incident management
Lessons from the Trenches

• “Operationalizing” assessment of incidents involving PII and PHI
  • Becoming a necessity due to frequency of incidents and complexity of regulations
  • Must carry out tasks presuming the need to “prove” your decisions/outcomes as to compliance
  • Will grow in complexity as you add in Accounting for Disclosure of authorized disclosures, added to unauthorized ones
Forecast

- Increased scrutiny & enforcement will continue
- Business associates will grow in prominence relative to protecting PHI
- Trends (cloud, mobile, EHRs/HIEs) are pointing towards higher velocity of incidents & increased importance of managing them properly
Resources

• PHI Protection Network (PPN) LinkedIn Group
  http://www.linkedin.com/groups/PHI-Protection-Network-PPN-4493923

• 2012 Ponemon Study on Patient Privacy & Data Security
  http://www2.idexpertscorp.com/ponemon2012/

• 3 Steps to Tackle HIPAA’s Final Rule
  http://www2.idexpertscorp.com/resources/BestPracticesChecklists/3-steps-to-tackle-hipaas-final-rule/

• HIPAA Final Omnibus Rule Whitepaper
  http://www2.idexpertscorp.com/omnibus-hipaa-final-rule-whitepaper/

• HIPAA Final Omnibus Rule Playbook: Covered Entity Edition
  http://www2.idexpertscorp.com/resources/BestPracticesChecklists/hipaa-final-omnibus-rule-playbook/

• HIPAA Final Omnibus Rule Playbook: Business Associate Edition
  http://www2.idexpertscorp.com/resources/BestPracticesChecklists/hipaa-final-omnibus-rule-playbook-ba/

• RADAR Software for Healthcare Entities
  http://www2.idexpertscorp.com/data-breach-tools/radar-for-phi/

• Medical Identity Fraud Alliance:
  http://www.medidfraud.org