Best Practice for a Healthcare Data Breach: What You Don’t Know Will Cost You

This roundtable discussion is brought to you by Experian® Data Breach Resolution, Stroz Friedberg, and AHLA’s Health Information and Technology (HIT), and is co-sponsored by the Hospitals and Health Systems (HHS) In-House Counsel (In-House) Payors, Plans, and Managed Care (PPMC), and Physician Organizations (Physicians) Practice Groups.

May 18, 2011 · 2:30-3:30 pm Eastern

Moderator:
Tony Hadley
Sr. Vice President of Government Affairs & Public Policy
Experian

Speakers:

Paul Luehr
Managing Director & General Counsel
Stroz Friedberg

Emilio Cividanes
Partner and Co-Chair
Regulatory Practice Group
Venable LLP
Tony Hadley, Moderator
Experian

- Senior Vice President, Government Affairs & Public Policy

- Leads the corporation's efforts in communicating to government officials at all levels about Experian's business operations and regulatory regimes.

- Interprets governmental policy and regulatory requirements and informs Experian executives about requirements and trends associated with the collection, use and processing of data.

- Areas of expertise include credit reporting, financial fraud, financial risk analysis, identity management, cross-channel consumer marketing, e-commerce and data protection.
Agenda

- **Webinar Objectives:**
  - A strategic breach response plan is the best means for preventing a healthcare data breach
  - Laws and regulations governing companies that collect and use healthcare and medical information
  - Steps to take during the first 72 hours of a breach incident

- **Webinar Overview:**
  - Two of the nation’s top legal experts on data breach law will share specific and detailed advice in this evolving field of law

- **Questions and answers**
Emilio Cividanes
Venable LLP

- Co-chairs the Regulatory Practice Group of Venable LLP

- One of the first privacy lawyers in the nation, and a member of the team recognized by both Computerworld and Chambers USA for its outstanding privacy and data security practice.

- Has assisted companies in connection with more than 100 data security incidents, ranging from health data to credit cards to Social Security Numbers.

- Successfully represented companies in connection with privacy and security-related litigation and congressional and regulatory investigations, including serving as lead counsel in defending Reed Elsevier Inc. in connection with the FTC's 3-year investigation of the company's data security practices.
Paul H. Luehr
Stroz Friedberg

- Managing Director, Chief Privacy Officer, and General Counsel of Stroz Friedberg.

- Served eleven and a half years as a federal attorney with the U.S. Department of Justice (DOJ) and the Federal Trade Commission.

- He was involved in the post-9/11 search of terrorist Zacarias Moussaoui’s laptop and was also featured by Business Week as one of the nation’s top cyber-cops.

- He leads the Healthcare Data Breach practice for Stroz Friedberg. As an incident response expert, he has helped resolve a variety of breach matters on behalf of pharmaceutical companies, university research facilities, medical device manufacturers, health insurance companies, and other healthcare entities.
Legislative and Regulatory Agenda

- No single federal law or regulation governs the security of all types of sensitive information.

- Several States require, or are considering requiring special protection for health information.

- State laws are not limited to healthcare providers, but may affect any employer or other entity with computerized employee benefits or other health data.

- In Congress, the Kerry/McCain privacy bill would exceed HIPPA in its treatment of consumer data related to “medical conditions.”
Medical Data Breaches Are Common

- Mar. 2011—Info. of 2,777 patients lost from Detroit hospital on misplaced flash drive
- Feb. 2011—NYC Health and Hospitals Corp. filed a lawsuit against a vendor after electronic files containing info. for 1.7 million patients stolen from unlocked van
- Oct. 2010—IN AG sued WellPoint for delaying to notify his office and 32k customers of a data breach
- Sept. 2010—CA imposes maximum $250k fine on Stanford Children’s Hosp. for late disclosure of breach affecting 532 patients
- Sept. 2010—33k patient records stolen from LA hospital and sold for value of recycled paper
- Jan. 2010—CT sues Health Net re: data of 446,000 patients lost when server drives go missing
Medical Data Breaches Are Costly

- A 2010 study concluded that breaches cost the healthcare industry about $6 billion per year.
- A separate 2011 study indicates that the total economic impact of medical identity theft is $30.9 billion annually, up from $28.6 billion in 2010.
- The 2010 study found that health care firms spend about $1 million per year, per firm, on data breaches.
- Data breaches can result in an estimated $107,580 in revenue losses from patients choosing other facilities for the rest of their lives.
- Of the healthcare facilities surveyed, 69% had insufficient policies and procedures to thwart a data breach and detect the loss of patient data and 70% of hospitals did not find protecting patient data a priority.
Prevention Is the Best Medicine!

- All facilities who maintain patient data or personal data about individuals should have a data breach incident response plan in place.
- Having a data breach incident response plan in place will help guide your organization’s proactive response to any incident.
- Penalties are often imposed on organizations for delayed or late notification to individuals. An incident response plan can promote a timely response.
Incident Response Plans
What Should Your Incident Response Plan Contain?

- Designated incident lead
- Emergency contacts
- Internal reporting system to alert legal, senior management, communications, and others
- Information on relevant regulatory and law enforcement agencies that must be contacted
- Steps required to assess scope of breach and preparation of response
Designated Incident Lead

- One individual (and backup) designated to coordinate the response
- Should act as go-between for management and the response team
- Typically someone from Legal or Chief Privacy Officer
- Will coordinate efforts among all groups, notify appropriate people within the company and externally, document the response, identify key tasks and estimate costs
Emergency Contacts and Internal Reporting System

- Emergency Contact List should include
  - Representative(s) of executive management team
  - Legal, privacy & compliance
  - Operations (Security & IT)
  - Customer Service and/or HR
  - Communications/Public Relations
  - Outside Experts

- Incident Response Plan should designate structure of internal reporting system
Law Enforcement Agencies

- If you believe the incident may have involved illegal activities, notify law enforcement of the breach.
- Incident response plan should include contact info.
- Key law enforcement may include:
  - FBI
  - U.S. Secret Service
  - Local law enforcement
Assessing the Breach and Response

Incident Plan should contain steps necessary to contain the breach and to conduct a preliminary internal assessment of the scope of the breach. Consider:

- Isolating the affected system to prevent further release;
- Activating auditing software;
- Preserving pertinent system logs;
- Making back-up copies of altered files to be kept secure;
- Identifying systems that connect to the affected system;
- Retaining an external forensic expert to assist with the investigation;
- Documenting conversations with law enforcement and steps taken to restore the integrity of the system.
Assessing the Breach and Response, cont.

- Incident response plan should contain steps to undertake to provide prompt notice to affected individuals, if required

- Be aware of the following:
  - HITECH Act impose timetables on providing notice, some states do also;
  - HITECH Act and some states specify the contents of the notice;
  - There may be requirements to notify HHS Secretary, specific government authorities and/or credit bureaus;
  - There may be requirements regarding method of notice.
Assessing the Breach and Response, cont.

- Incident response plan should also contain guidelines to assess when the following may be required:
  - Notification to other third parties, such as insurance carriers, card holder associations, etc.;
  - Provision of an identity theft protection service, identity theft counseling and professional assistance;
  - Press strategy and press responses;
  - Public affairs and government affairs strategy.

- Incident response plan should also contain a plan post-notification to review events and make adjustments to technology and response plan to reflect lessons learned.
Laws and Regulations Governing Data Breach
What the HITECH Act Requires

- The HITECH Act requires notification when unsecured protected health information is accessed, acquired, used, or disclosed without authorization, i.e., during a “breach.”
State Laws That Govern Breach Notification

State breach notification laws (now in 46 states, DC, PR, and USVI) generally require notification to individuals if their “personal information” was, or reasonably is, believed to have been acquired by an unauthorized person.

- “Personal information” is commonly defined to include an individual’s name combined with a certain “data element” such as a Social Security number, driver’s license number, or account number in combination with any password that would permit access to a person’s account.
- State laws can have significant and conflicting variations.
- Arkansas, California, Delaware and Missouri include medical information in their state data breach laws.
- Patient records often include SSN# and other data that might be captured by state law.
FTC Rule and “Dual Role” Entities

- Federal Trade Commission issued similar (but not identical) notification rule for:
  - Vendors of “personal health records”
  - Entities related to vendors of personal health records
  - Third party servicers of these vendors and related entities

- Some entities may play “dual role”; agency jurisdiction depends on role in which company suffered breach
State Law Preemption

- HHS notification standard preempts “contrary” state laws
- “Contrary” means entity could find it impossible to comply with both, or state law is obstacle to realizing federal law’s purpose
- In many cases, compliance with both federal and state laws will be required
Notification Under The HITECH Act

- “Unsecured” means any information not secured through encryption or destruction, in accord with HHS guidance.

- “Protected health information” (PHI) retains same meaning as under HIPAA:
  - Individually identifiable health information
  - Relates to health condition, treatment or payment
  - Transmitted or maintained in any medium

- What is a breach?
  - Unauthorized acquisition, access, use or disclosure of PHI that compromises security or privacy of PHI
  - “Unauthorized” means not permitted by HIPAA Privacy Rule
  - “Compromises security or privacy” means that unauthorized action poses significant risk of financial, reputational or other harm
When to Notify?

- Notify “without unreasonable delay” and no later than 60 calendar days after breach is discovered
  - FL and OH notification laws require notice w/in 45 days
- Deadlines for breach at business associate depend on relationship:
  - If Business Associate is independent contractor, deadline runs from time business associate notifies covered entity
  - If Business Associate is agent of Covered Entity, deadline runs from Business Associate’s discovery of breach
- May delay notification if law enforcement provides documented statement that notice would harm national security or impede criminal investigation
When is a Breach Discovered?

- “Discovery” means first day breach is known, or reasonably should have been known, to any employee, officer, or agent of company

- Knowledge of breach by any employee can trigger notification deadlines for the company

- Company should have in place:
  - Reasonable systems for detecting breach
  - Mechanisms to ensure that any employee who discovers breach reports to management
What is Not a Breach?

- If de-identified information is disclosed
- If you believe, in good faith, that the unauthorized person could not reasonably have retained information
  - In a few states “unauthorized access” alone is enough to trigger notification
- If workforce member accesses information without permission but in good faith, as long as there is no further unauthorized action
- If workforce member reveals information to an unauthorized colleague, as long as there is no further unauthorized action
Whom to Notify?

- Business Associate must notify covered entity
  - Business Associate may also notify individuals directly, if arranged by contract
- Covered entity, in turn, must notify
  - Individuals whose information is reasonably believed to have been accessed, acquired, used or disclosed without authorization
    - Notify next of kin or personal representative, if affected individual known to be deceased
  - Secretary of Health and Human Services
    - Certain states require state gov’t agencies to be notified, i.e., NYAG
  - Media notice, in some cases
Individual Notification Methods

- Via first-class mail
- Via e-mail, if individual has agreed to e-mail notice and has not withdrawn agreement
- **If contact information insufficient**, then update information or provide substitute notice:
  - For fewer than 10 people, can use telephone or other method
  - For 10 or more people, either notify major media outlets or post on website homepage for 90 days
  - *Almost all states permit substitute notice if individual notice is particularly burdensome in terms of cost or number of individuals, often described as over 500k individuals and/or costing more than $250k*
- Urgent notice (telephone) may be required in some cases
Individual Notification Contents

- Must use plain language
- Must include, to the extent possible:
  - Description of breach
  - Dates of breach and discovery
  - Description of types of information involved
  - Steps individuals should take
  - Steps entity is taking to respond to breach
  - Contact information for questions
- Some states specify particular language to be included in notice. For example, MD requires toll-free numbers and addresses for credit reporting agencies, toll-free numbers, addresses, and websites for the FTC and state AG, and a statement that the individual can obtain information from these sources about steps to avoid identity theft.
HHS and Media Notification

- If breach affects 500 or more individuals nationwide, must notify HHS Secretary at same time as individuals
- For breaches that affect under 500 individuals, submit annual log to HHS Secretary
- Media notice required for any breach that affects 500 or more individuals in a single state or jurisdiction
- This required media notice is different from substitute notice provided if contact information is insufficient
The First 72 Hours

- Execute Your Plan
  - Follow your Escalation Protocol
  - Assemble your Team

- Respond to the Breach—
  MOVE QUICKLY & DOCUMENT YOUR WORK AS YOU:
  - Preserve the Evidence
  - Identify the Comprised Data
  - Communicate Progress
Assemble your Team
Preserve the Data – Lost or Stolen Media

- Secure premises
- Take inventory of missing items and their locations
- Review keycard and surveillance data for unusual activity
- Conduct on-site investigations
  - Law enforcement
  - Private security experts

Key cards
Video surveillance
Fingerprints
Preserve the Data – Lost or Stolen Media

- Locate formerly connected media
- Locate backups or “cousin” data
Preserve Compromised Data

- Take infected machines offline
  - LEAVE POWER ON!
  - DO NOT POKE AROUND!
  - INSERT CLEAN & PATCHED MACHINES

- Call forensic experts to image data

- Save off-log files (e.g. web, firewall, IDS)

- Pull backups out of rotation
Identify the Compromised Data

- Interview key custodians
  - With Legal, HR, IT, Forensics

- Focus on PHI/PII
  - Patient or customer data
  - Employee data

- Verify with Forensics
Expert Technical Incident Response Team

- **Counsel**
- **EXPERT IR Team Lead**
- **IT Leader**
  - **Evidence Team Lead**
  - **Forensic Analysis Team Lead**
  - **Malware Analysis Team Lead**
    - **Hard drive & log acquisition**
    - **Volatile data preservation & triage**
    - **Media analysis**
    - **Network log analysis**
    - **Static & dynamic analysis**
    - **Reverse engineering & antidote**
Identify the Compromised Data - Forensics

- **Volatile Data Capture**
  - Capturing physical memory may reveal processes not normally seen by user or IT
Identify the Compromised Data - Forensics

- Deleted Hacker Tools
  - What data was targeted?
  - How was data exfiltrated?
  - Was data accessed, acquired, used?

What is the Risk of Harm?
Identify the Compromised Data - Forensics

- Consolidate Data
  - By location
  - By file type
  - By type of PHI/PII

- Account for Variations

- Align with Names
Communicate Progress

- **Audience**
  - Team Members – Outside & In-house Counsel, Compliance, HR, IT, Business Managers, Public Affairs, Experts
  - Board/CEO, Executives
  - Business Partners
  - Regulators – HHS, AGs, State Health/Ins., FTC
  - Employees
  - Shareholders
  - Patients or Customers

- **Difficult Issues**
  - Certainty – data taken; victims affected
  - Timing – date of breach; when clock starts
Case Study

Theft of Backup Tapes

- 7TB of data missing
- Previous week’s backup used as authoritative source
- Encryption did not save the day
- Culled data 99.8% through forensic analysis (server, file, keyword)
- E-discovery platform used to search remaining 18GB
- Bulk of sensitive information was employee data, not PHI
Thank You!

Audience Questions & Answers
Preparing for a Healthcare Data Breach: What you don’t know can cost you © 2011 is published by the American Health Lawyers Association. All rights reserved. No part of this publication may be reproduced in any form except by prior written permission from the publisher. Printed in the United States of America.

Any views or advice offered in this publication are those of its authors and should not be construed as the position of the American Health Lawyers Association.

“This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering legal or other professional services. If legal advice or other expert assistance is required, the services of a competent professional person should be sought”—from a declaration of the American Bar Association