April 25, 2013

Incident Response and Data Breach in the HealthCare Sector

Sheppard Pratt Conference Center
6501 N Charles St,
Towson, MD 21204

Mark D. Rasch, Esq.
Mark@MarkDRasch.com
(301) 547-6925
Health Care Industry Is A Primary Target For Thieves and Regulators

- Represents one of the largest global repositories of sensitive personal information
- All services targeted
  - Health Care Providers
  - Health Services
  - Life Sciences
  - Health Insurance
- Regulators require
  - Controlling access to patient medical and personal data
  - Transaction accountability
71 percent of health care organizations suffered a data breach in the last year.

Data breaches in US alone Cost between $4.2 billion and $8.1 billion a year, or an average of $6.5 billion.

Most breaches were the result of employees losing or having their IT devices stolen or other unintentional, but ill-advised, employee action according to 49 and 41 percent of respondents.

Shoddy security from partners and providers, including business associates, according to 46 percent of participants, was another significant reason.

Once a breach is discovered, 83 percent of hospitals reported it taking one to two months to notify affected patients. Nearly a third, or 29 percent, admitted that breaches lead to cases of identity theft, up 26 percent from the previous year.

Source, Dec. 2011, Second Annual Benchmark Study on Patient Privacy and Data Security conducted by the Ponemon Institute and sponsored by ID Experts.
Summary of Health Industry Challenges

- **Security**
  - Protecting Data and the “Brand”
  - Controlling access
  - Enforcing policies

- **Business Enablement**
  - Fast and secure access to patient records for clinicians
  - Integrate with clinical workstations and network access points
  - Access to information by external users
  - Interoperability with health information exchanges

- **Compliance Management**
  - Who has access to what, prove it, enforce it, and monitor it
  - Segregation of duties
  - Creating and managing user identities
  - Audit Reporting
  - Access Reporting
  - Breach Notification
Healthcare Security—a Growing Need

Security-Maturing
- RFID
- Medical Devices
- Medical Imaging
- Data leakage protection
- Identity & access mgmt
- Security infrastructure
  - Cyber security
- Application security
- Network security
- Single sign-on

Security-Becoming Priority
- Authentication
- Intrusion prevention
- User provisioning
- Data leak protection
- Desktop virtualization
  - Single sign-on
- Identity & access mgmt
- Mainframe security
- Cyber security
- Application security
- Network security

Security-Emerging
- Identity & access mgmt
- Data leakage protection
  - Malicious attacks
- Cyber security
- Web single sign-on

- Electronic billing protection
- Social networking privacy
- Patient monitoring security
  - Authentication
  - Intrusion prevention

- Smart cards
- Identity Management
- Fraud detection
Top Threats/Trends to HealthCare

1. Cloud
2. Mobility – broadly defined. Includes physician remote access (from home, etc.)
3. Social Media
4. Access Devices
5. Medical Devices
6. Complexity
7. Data Transfer
8. Data Access
9. Data Mining and Manipulation
10. Government Regulation (BA and AG)
11. Interoperability
12. General Threats – virus, malware, etc
Global Threats and Compliance

- General Themes
  - Complexity
  - Interoperability
  - Data as Asset - EHR
  - Data for Patient Outcome
  - Greater Regulatory Scrutiny
    - State Attorney’s General
    - Less Understanding of HIPAA/HITECH
- Changing Business Environment
  - Outsourcing/Offshoring
  - Telemedicine broadly defined
26 percent of organizations have yet to conduct a risk assessment.

43 percent grade their ability to counter information security threats as poor, failing or in need of improvement.

Less than half have a defined information security budget.

Respondents reported that their top information security priority for the next year is improving regulatory compliance efforts.
Maturity of the Security Environment: Average security 4.23 out of 7
Security Budget: Most below 3% IT budget on security (but increasing)
Oversight of Information Security: ½ have (CSO) or (CISO) or full-time staff in place to handle their organizations’ security functions
Employee/Patient Data Access: Almost all monitor most with Role-based and user-based controls. 2/3 give access to patients/surrogates.
Audit Logs: Yes they do.
Security in a Networked Environment: 82% share PHI with third parties (including government)
Future Use of Security Technologies: Main goals (a) identify data loss prevention, (b) e-mail encryption and (c) single-sign on
Patient Identity: Most respondents reported that their organizations’ validate the identity of patients at the time of a patient encounter (gov’t ID)
Medical Identity Theft: 14% had at least one known case of medical identity theft reported by a patient in the previous 12 months.

Budget Priorities in Healthcare

Percent of IT Budget Dedicated to Information Security

- Less than One Percent: 18%
- One to Three Percent: 35%
- Four to Six Percent: 16%
- Seven to 12 Percent: 3%
- More than 12 Percent: 4%
- Don't Know: 23%

Risk Analysis

Frequency of Conducting a Formal Risk Analysis

- Every Six Months: 8%
- Annually: 49%
- Every Two Years: 21%
- Every Three Years: 2%
- As Needed: 1%
- Other: 9%
- Don't Know: 10%

Mobile Monitoring

- Number of patients monitored by mobile networks to rise to 3 million by 2016, according to a new report on the mHealth sector from Juniper Research.
  - monitoring of cardiac outpatients is leading the field, as insurance reimbursement in the U.S. market plays a key role.
  - management of diabetes and COPD increasing
- Mobile Healthcare and medical app downloads will reach 44 million in 2012, rising to 142 million in 2016
- Need FDA clarification on whether apps are “devices.”
- EHR access increasing
Liability Concerns

- Litigation (Privacy and Security)
  
  *In re iPhone Application Litigation (2011)* Plaintiffs alleged that Apple and mobile ad networks unlawfully allowed third party apps to collect personal information without user consent or knowledge. Issue was damages.

  *Claridge v. RockYou, Inc.* (N.D. Cal. 2011) Defendant failed to secure user data, allowing hacker to have access to 32 million usernames and passwords – Issue was “value” of personal information.

  *Fraley v. Facebook* (N.D. Cal., Dec. 19, 2011) Plaintiffs alleged that Facebook unlawfully appropriated its user’s data through its Sponsored Stories marketing program.

  *Villegas v. Google* (complaint filed Feb. 28, 2012) Plaintiffs allege that Google and Point Roll were exploiting a gap in the Safari and IE browsers to circumvent a user’s cookie settings.

  *Gaos v. Google* (N.D. Cal. Mar. 29, 2012) Google allows website owners (and third parties) to see user-submitted search terms, which can be linked to user through re-identification.
Recent Breaches

- Massachusetts Eye and Ear Infirmary 2010 theft of unencrypted laptop.
  - Settlement Sept 2012 $1.5 million penalty, a corrective action plan to review, revise, and maintain policies and procedures to ensure compliance with the HIPAA Security Rule. Plus, the agreement requires that an independent monitor conduct assessments of compliance with the corrective action plan and submit semi-
January 18, 2013 - Utah Department of Health suffered breach of 6,000 Medicaid patients when an employee of contractor, Goold Health Systems, misplaced a USB device while traveling. This is the UDOH's second data breach in less than a year. In April, the department suffered a data breach that affected nearly 800,000 individuals when hackers compromised its server system.

January 2, 2013. Hospice of North Idaho settled a 2010 security case by agreeing to pay $50,000 to HHS. The case stemmed from a stolen laptop with unencrypted data containing the protected health information of 441 patients.

December 26, 2012. Personal health information on approximately 4,000 patients treated by the University of Michigan Health System breached when equipment containing the information was stolen from the car of an employee who works for Omnicell, a hospital vendor. The device was not secured, which is a violation of the company's standard policies.
PLANNING AND PREPARATION
- Policy review or development
- Installation and monitoring of forensic appliances for remote forensics (e.g., EnCase)
- Training for Employees
- Training for IT Staff
- Cyber and casualty insurance review and evaluation
- Legal and Regulatory Compliance Review (for laws and regulations that mandate incident response services)
- Network mapping and validation
- Information Security Assessment Services
- Electronic Discovery Readiness Review
- Ongoing Monitoring for Breaches
- Crisis Communications Training and Support

MANAGEMENT
- Crisis management or support services
- Crisis Communications Services
- Information Security Regulatory Compliance Services
- Privacy Impact Review During Incident
- Inside and Outside Counsel Coordination
- Vendor and Supplier Coordination
- Incident Response Escalation

SUPPORT
- Consumer Mitigation Services (credit repair services, credit freeze, credit reporting services)
- Data Breach Remediation and Repair
- Electronic Discovery and Document Review
- Data Breach Notification Services
- SEC Disclosure Support
- Regulatory Reporting Support
- International Coordination Support
- Privacy and Financial Impact Assessment

POST INCIDENT OPERATIONS
- Post-incident forensic services
- Physical security e
- Cyber insurance claims coordination and presentation
- Validation and Certification Services
- Litigation Support Services
- Expert Witness Services
- Privacy Consulting and “Chief Privacy Officer” Services (during or post-incident).
- Disaster Recovery and Business Continuation Planning.
- Cloud-based or outsourced data backup or recovery

INVESTIGATION
- Digital Investigative Services
- Computer Forensic Investigation
- CERT/ISAC Coordination
- Forensic data recovery
- Analysis of forensically obtained data
- Computer Security Consulting Services
- Coordination with Law Enforcement and Regulatory Agencies in connection with incidents
- Forensic data storage and evaluation (large scale data analysis)
- Network and log data collection and review
- Discovery and litigation assistance for investigation
- EnCase Deployment

Effective Incident Management
Data Breach Notification Requirements

- 48 States have data breach notification laws
- FTC/GLBA Data Breach Notification
- EU Data Breach Notification (New)
- HIPAA/HITECH Data Breach Notification
- All differ in what is a breach
- What is “personal data”
- When and to whom to report
- How to report
- How to track reporting
- Interplay between state law and SEC/Federal/International
- May also require remediation (credit freeze, credit reporting, etc.)
- PCI DSS requirements
- Admission of Liability
HHS HIPAA/HITECH Final Rule

- Modifies the definition of "breach" and the risk assessment approach
- The rule eliminates the "harm threshold" provision, which allowed covered entities and business associates to avoid breach notification if they determined themselves a breach would not cause harm to an individual. HHS now calls for covered entities and BAs to assess the probability that the PHI has been compromised instead of assessing the risk of harm to the individual.
  - an impermissible use or disclosure of PHI is "presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised."
- Replaces the "significant risk of harm" standard set forth in the Interim Final Rule. HHS notes that the prior focus on "harm to an individual" was too subjective, risking inconsistent interpretations and results across covered entities and business associates.
- Requires a post-breach assessment of probability that PHI has been compromised
Breach Defined

- An **impermissible use or disclosure** of protected health information is **presumed to be a breach** unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised.

- Covered entities and business associates have the **burden of proof** to demonstrate that all notifications were provided or that an impermissible use or disclosure did not constitute a breach (such as by demonstrating **through a risk assessment** that there was a low probability that the protected health information had been compromised) and must **maintain documentation** sufficient to meet that burden of proof.
No more “harm standard” – Risk Assessment

- New rule removes the “harm standard” and modifies the risk assessment to focus on the risk that the protected health information has been compromised.
- Breach notification is not required under the final rule it is demonstrated
  - through a risk assessment
  - that there is a low probability that the protected health information has been compromised,
  - rather than demonstrate that there is no significant risk of harm to the individual.
- Objective factors covered entities and business associates must consider when performing a risk assessment to determine if the protected health information has been compromised and breach notification.
Statutory exceptions

- Sometimes the unauthorized acquisition, access, use, or disclosure of protected health information is so inconsequential that it does not warrant notification.

- if a covered entity misdirects a fax containing protected health information to the wrong physician practice, and upon receipt, the receiving physician calls the covered entity to say he has received the fax in error and has destroyed it, the covered entity may be able to **demonstrate after performing a risk assessment** that there is a low risk that the protected health information has been compromised.

- BUT – the rule requires that this still be assessed against standards
After possible breach, **must conduct a risk assessment** that considers at least the following factors:

1. the nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
2. the unauthorized person who used the protected health information or to whom the disclosure was made;
3. whether the protected health information was actually acquired or viewed; and
4. the extent to which the risk to the protected health information has been mitigated.

Must provide documentation of the assessment and validation of conclusions.

Burden of proof is on covered entity or business associate

May make a NOTIFICATION without conducting the assessment.
Consider types of identifiers and the likelihood of re-identification of the information.

Is the information of a more sensitive nature.
- financial information (credit card numbers, social security numbers, or other information that increases the risk of identity theft or financial fraud.)

Clinical information
- the nature of the services or other information
- the amount of detailed clinical information involved (e.g., treatment plan, diagnosis, medication, medical history information, test results).
- Probability that the protected health information could be used by an unauthorized recipient in a manner adverse to the individual or otherwise used to further the unauthorized recipient’s own interests.
To Whom Was Information Improperly Disclosed?

- Does the unauthorized person who received the information have obligations to protect the privacy and security of the information?
- If protected health information is impermissibly disclosed to another entity obligated to abide by the HIPAA Privacy and Security Rules or to a Federal agency obligated to comply with the Privacy Act of 1974 and the Federal Information Security Management Act may not have to make disclosure.
- Does the unauthorized person have the ability to re-identify de-identified information or data sets?
- Remember, “breach” includes BOTH unauthorized access or unauthorized use.
Breach Investigation is REQUIRED

Must determine if the protected health information was **actually acquired or viewed** or, alternatively, if only the opportunity existed for the information to be acquired or viewed.

**Example 1**: Laptop computer is stolen and later recovered and a forensic analysis shows that the protected health information on the computer **was never accessed, viewed, acquired, transferred, or otherwise compromised**, the entity could determine that the information was not actually acquired by an unauthorized individual even though the opportunity existed.

**Example 2**: Covered entity mails information to the wrong individual who opens the envelope and calls the entity to say that she received the information in error. The unauthorized recipient viewed and acquired the information because she opened and read the information to the extent that she recognized it was mailed to her in error.

**Example 3**: Covered entity mails information to a patient's old address, faxes information to the wrong number, leaves a voice message at the wrong number reminding a patient of an upcoming appointment, or, in situations where patients have identical or similar names, contacting the wrong patient to inform him or her that lab results were ready. Investigation required.
Mitigating Factors

Consider the extent to which the risk to the protected health information has been mitigated.

- obtaining the recipient’s satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means) or will be destroyed,

- consider the extent and efficacy of the mitigation when determining the probability that the protected health information has been compromised.

Do you trust the assurances?

Employee? Affilliate? Independent third party?

The recipient of the information will have an impact on whether the covered entity can conclude that an impermissible use or disclosure has been appropriately mitigated.
**Limited Data Set - Changes**

- Prior rule – if limited data set breached, no notification required.

- New rule - Removed the exception for limited data sets that do not contain any dates of birth and zip codes.

**NOW**

- following the impermissible use or disclosure of any limited data set, a covered entity or business associate **must perform a risk assessment** that evaluates the factors discussed to determine if breach notification is not required.

- Presumably the fact that it is a limited data set goes to the issue of nature and extent of PHI breached
Encryption is your friend...

- If protected health information is appropriately encrypted then no breach notification is required following an impermissible use or disclosure of the information.
- BUT NOTE: Since the new rule applies to both improper disclosure and improper USE, an improper USE of information that is encrypted at one time may constitute a breach. An authorized person using PHI for an improper purpose is now a breach.
- Rule refers specifically to Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (74 FR 42740, 42742).
- Another caveat – the regulation does not exempt unencrypted data that may be difficult or even impossible to recreate because of time, expense, special equipment needed, special software needed, etc. “unsecured protected health information” as “protected health information” that is not secured through the use of a technology or methodology specified by the Secretary in guidance...”
Notice of Privacy Practices

- What do you have to say about breach of incident response?
- What do you have to say about breach investigation?
- Required to notify patients of the circumstances of a breach, as well as what steps individuals should take to protect themselves from potential harm resulting from the breach.
Data Breach and "Minimum Necessary"

- Privacy Rule’s “minimum necessary” standard requires a covered entity to make reasonable efforts to limit access to protected health information to those persons or classes of persons who need access to protected health information to carry out their duties and to disclose an amount of protected health information reasonably necessary to achieve the purpose of a disclosure.

- Same standard on business associates and subcontractors

- Failure to make such efforts, or failure to enforce such efforts then result in an “unauthorized use” of information even though an authorized person has access to records. **If person has access to TOO MUCH information (more than they reasonably need) this is a DATA BREACH under the new rules.**

- Risk Assessment is then REQUIRED, and breach notification may be required.
When is a breach “discovered?”

- Section 164.404(a)(2) Breach shall be treated as **discovered** by a covered entity
  - on the first day the breach is **known to the covered entity**, or by exercising reasonable diligence **would have been known** to the covered entity.
  - “reasonable diligence” defined to mean the “business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.”

- Do you “know” what any employee knows?
- Do you “know” what any agent or subcontractor knows? (common law of agency)

- Rule is when the ENTITY knows, NOT when management knows. Thus, having incident response, incident identification and escalation is critical.
  - “We encourage covered entities and business associates to ensure their workforce members and other agents are adequately trained on the importance of prompt reporting of privacy and security incidents.”
Following a breach of unsecured protected health information covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. In addition, business associates must notify covered entities that a breach has occurred.

Individual Notice

- first-class mail or e-mail if the affected individual has agreed to receive such notices electronically.
- without unreasonable (in no case later than 60 days following the discovery of a breach)

Include

- description of the breach,
- description of the types of information that were involved in the breach,
- steps affected individuals should take to protect themselves from potential harm,
- what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity.
Breach notices, to the extent possible, must include:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
2. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
3. Any steps individuals should take to protect themselves from potential harm resulting from the breach;
4. A brief description of what the covered entity involved is doing to investigate the breach, mitigate the harm to individuals, and to protect against any further breaches; and
5. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.
What will HHS review in terms of the extent of breaches in the new omnibus rule?
- Number of individuals affected
- Time period during which the violation occurred
- Nature and extent of the harm resulting from the violation, consideration of which may include but is not limited to:
  - Whether the violation caused physical harm
  - Whether the violation resulted in financial harm
  - Whether the violation resulted in harm to an individual's reputation
  - Whether the violation hindered an individual's ability to obtain healthcare
- Prior indications of non-compliance
Chairman Levitt first proposed mandatory reporting of incidents, threats and vulnerabilities in 2002 – Industry pushback

SEC Guidance issued October 2011

Risk factors – Incidents AND Vulnerabilities
- Description of outsourced functions that have material cybersecurity risks;
- Description of cyber incidents experienced by the registrant that are material, including a description of the costs and consequences; and
- Description of relevant insurance coverage for cyber incidents.

MD&A
- Cost
- Business
  - If there has been an incident
- Legal Proceedings
- Financial Statements
**Business Associate/Contractual Security**

- HIPAA/HITECH requires Business Associate Agreement to protect PHI
- Industry Standard for ANY Outsourcing agreement
  - Cloud
  - PHI
  - PCI
  - PII
- Business Associate? Short answer – anyone who touches MY data or my customer data
- Sets out ALL security requirements
  - Security Standards
  - Auditing (third party, etc.)
  - Breach notification
  - Levels of care (uptime, DR/BCP)
BA’s and their subcontractors are now directly liable to HHS and Attorney’s General for compliance

We also continue to believe that, despite the business associate’s direct liability for certain provisions of the HIPAA Rules, the business associate agreement is necessary to clarify and limit, as appropriate, the permissible uses and disclosures by the business associate, given the relationship between the parties and the activities or services being performed by the business associate.

They must comply with data breach and security rules themselves

BA Agreements can specify how and when to notify the covered entity

BA’s must now have reasonable security AND incident response plans with training and awareness.
In the ordinary course of our business, we/we] [collect and] store sensitive data, including intellectual property, our proprietary business information and that of our customers, [suppliers and business partners,] and personally identifiable information of our [customers and] employees, in our data centers and on our networks. The secure [processing,] maintenance [and transmission] of this information is critical to our operations [and business strategy]. Despite our security measures, our information technology and infrastructure may be vulnerable to attacks by hackers or breached due to employee error, malfeasance or other disruptions. Any such breach could compromise our networks and the information stored there could be accessed, publicly disclosed, lost or stolen. Any such access, disclosure or other loss of information could result in legal claims or proceedings, [liability under laws that protect the privacy of personal information,] [and regulatory penalties,] [disrupt our operations [and the services we provide to customers],] [and] damage our reputation, [and cause a loss of confidence in our products and services], which could adversely affect our [business/operating margins, revenues and competitive position].
What Standard to Apply in Contracts?

- **CoBIT** - Control Objectives for Information and Related Technology by (ISACA) (not truly a security standard).

- **FISMA** (the Federal Information Security Management Act of 2002) references to NIST

- **ISO 27002** (formerly ISO 17799) (or subset) code of best-practice recommendations for information security management. It contains recommended information security controls and objectives in twelve areas (risk assessment, security policy, security organization, IT asset management, HR security, physical and environmental security, communications and operations management, access controls, information systems acquisition and maintenance, business continuity, and compliance with relevant laws and policies).

- **PCI-DSS**

- **SAS 70** (AICPA Statement on Accounting Standards No. 70: Service Organizations). This usually addresses preventive and detective internal security controls, as well as business continuity. The SAS 70 Type II audit requires an evaluation of the effectiveness of security controls over the review period, usually six or twelve months. The equivalent in the UK is the AAF 01/06 "assurance report" (replacing FRAG 21/94)
What is Security Incident Response?

- Security incident response is the ability to detect and resolve problems that threaten people, process, technology and facilities.
- Resolution of an incident through an appropriate reaction to, and containment of, the problem constitutes security incident response.
A Security Incident Response Team (SIRT) is formed to better address the dynamic threats against company systems and to handle security incidents by centralizing this activity in one functional unit.

A more formalized incident response team can better respond to security incidents and ensure that the broad range of issues which arise are fully coordinated.
How do I get started?

- Research and utilize well known resources
  - NIST SP800-61
  - SANS Institute
  - CERT
  - Department of Homeland Security
  - NSA
For More Information

Mark D. Rasch, Esq.
Mark@MarkDRasch.com
Tel: 301.547.6925