Locke Lord LLP

Accelerating Incident Response - HIPAA 2015

Theodore P. Augustinos
Ellen M. Giblin
David S. Szabo

Agenda

- Medical Identity Theft and Fraud
- Specific Healthcare Industry Concerns and Challenges for Incident Response
- The New Cyber Threat Environment and Corporate Data Governance Trends
- Questions (and maybe Answers)

Medical Identity Theft and Fraud

- Ellen M. Giblin, JD, M Ed, CIPP/US/G/C
- Counsel – Locke Lord LLP

Medical Identity Theft and Fraud

Medical Identity Theft is Big Business

The FBI has warned the healthcare industry that companies are being targeted by hackers, publicizing the issue following an attack on U.S. hospital group *Community Health Systems Inc.* that resulted in the theft of millions of patient records.

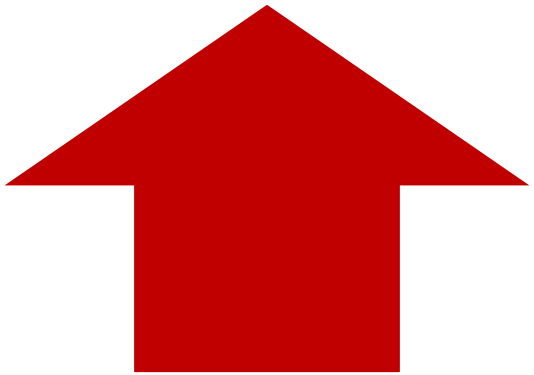
"These actors have also been seen targeting multiple companies in the healthcare and medical device industry typically targeting valuable intellectual property, such as medical device and equipment development data". (Reuters 2014)

Medical Identity Theft and Fraud *(Cont.)*

What is medical identity theft and fraud?

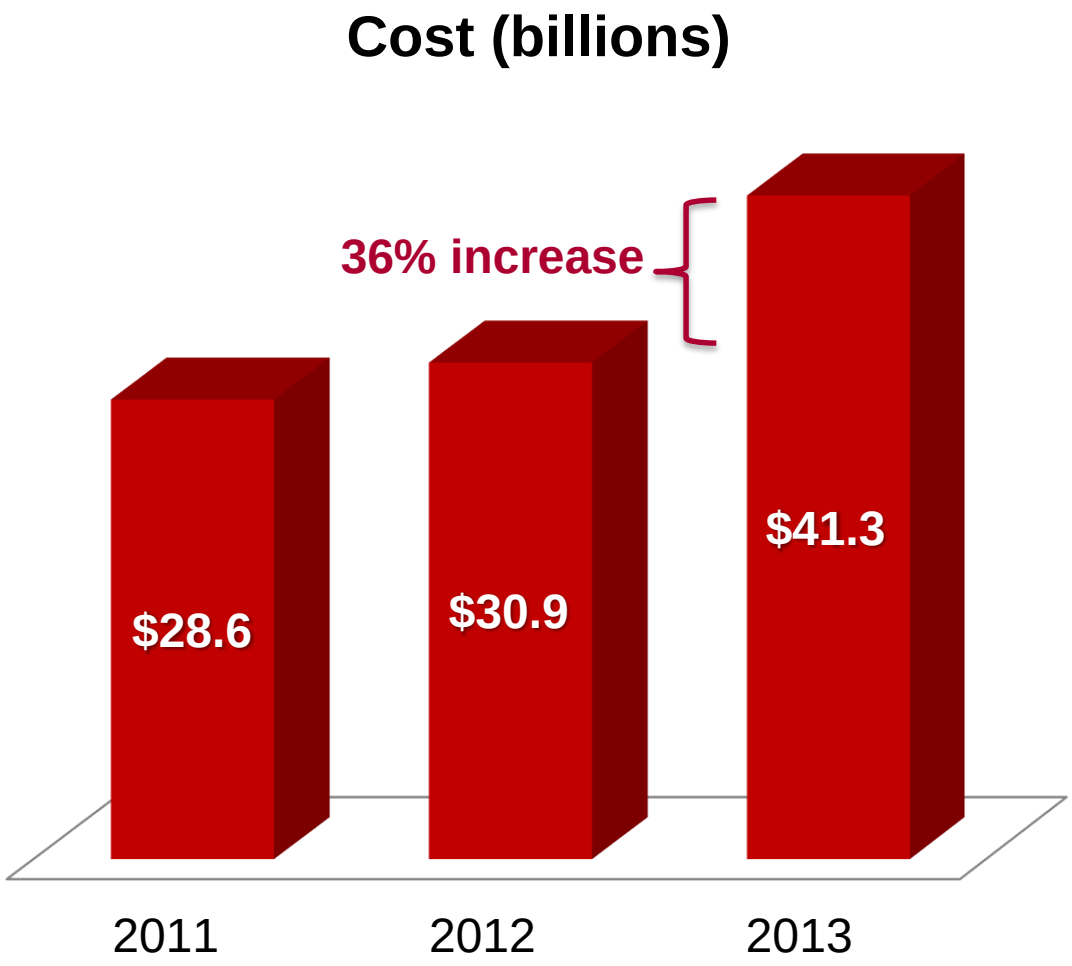
Medical identity theft occurs when someone steals a patient's Personally Identifying Information (PII) or Protected Health Information (PHI).

Medical fraud occurs when stolen PII or PHI is used in a way that allows personal gain by another. It can involve financial gain both from the sale or the use of PII to obtain medical goods and services or from filing false claims.



Medical Identity Theft and Fraud *(Cont.)*

Growing Impact of Medical Identity Theft



1.85 MILLION

Number of victims, 2013. Increase of 360,000.

$22,346

Average cost per victim. Up more than 10%.

75%

Percentage of consumers who are concerned about the privacy of their identity

Medical Identity Theft and Fraud *(Cont.)*

Medical Identity Theft and Fraud State Numbers

Rank	Total Fraud Incidents		Total Fraud ($ millions)		Incidents / Million People		Total Fraud ($ / Person)	
1	Florida	73	Florida	$2,002.2	Dist. of Columbia	4.64	Dist. of Columbia	$118.96
2	Texas	60	Texas	$773.1	Michigan	4.24	Louisiana	$117.82
3	Michigan	42	California	$768.1	Alaska	4.08	Alabama	$112.76
4	California	39	Michigan	$673.4	Florida	3.73	Florida	$102.40
5	New York	33	New York	$584.8	Louisiana	3.68	Colorado	$73.84
6	Illinois	23	Alabama	$545.1	Maryland	2.87	Michigan	$68.05
7	Pennsylvania	18	Louisiana	$545.0	Texas	2.27	South Carolina	$59.94
8	Louisiana	17	Colorado	$389.0	Kentucky	2.05	New York	$29.76
9	Maryland	17	South Carolina	$286.2	Illinois	1.79	Texas	$29.23
10	Georgia	15	Ohio	$150.7	Kansas	1.73	California	$20.04

Medical Identity Theft and Fraud *(Cont.)*

What those numbers mean in real life…

An Oregon hospital's billing department notified a pregnant woman that **someone had used her social security number to be treated for a crack overdose** at the ER of the same facility where she was about to deliver her baby.

In Washington, utilizing another woman's Social Security Number, a pregnant woman delivered a baby addicted to crack—and then abandoned the baby. **Police arrested the *victim* and put her children into protective custody.**

In Boston, a psychiatrist entered false diagnoses of psychiatric disorders into the records of individuals who were not his patients. **He did this to submit false bills to insurers.** One of the victims discovered a false diagnosis of severe depression when he applied for employment.

http://www.govhealthit.com/news/glimpse-inside-234-billion-world-medical-id-theft

Medical Identity Theft and Fraud *(Cont.)*

How Does This Impact Patient Care

- The damage can be potentially life-threatening to a patient:
  - Erroneous conditions and allergy information in record
  - Affects medical decisions made by patient caregivers
- Medical identity theft can disrupt patient welfare and credit rating.
- Victims of theft include:
  - Healthcare providers
  - Insurance companies
  - Patients
  - Consumers/Taxpayers

Medical Identity Theft and Fraud *(Cont.)*

Who is Fighting Medical Identity Theft & Fraud

- **Medical Identity Fraud Alliance (MIFA) -** The first public/private group uniting all stakeholders in jointly developing solutions and best practices for the prevention, detection and remediation of medical identity fraud.
- MIFA is dedicated to helping its members better protect their organizations and consumers from medical identity theft and the resulting fraud.
- Goal: Prevention, detection and remediation of medical identity fraud.

Medical Identity Theft and Fraud *(Cont.)*

How Can You Fight Medical ID Theft & Fraud

- Prevention
  - Prevent sharing or misusing Medicare & Social Security numbers.
  - Educate patients to the risks of medical identity theft and fraud.
- Detection - Do you:
  - Have a “Red Flags Program” in place to detect the signs of medical identity theft?
  - Respond to complaints about medical identity theft?
  - Detect errors and fraud with the use of technology?
- Mitigation – Do you:
  - Report lost, stolen or incorrect patient information?
  - Have clear policies for correcting corrupted records?
  - Encourage victims to check their credit reports?
  - Have an incident response plan for reporting cases of actual and suspected medical identity theft?

Medical Identity Theft and Fraud *(Cont.)*

Criminal and Internal Investigations:

- Who should conduct in your organization?
- What federal and state laws are implicated?
- Who should report medical identity theft and fraud to law enforcement?
- What other regulators must be given notice?
- Where in your Incident Response Plan have you assigned this responsibility?

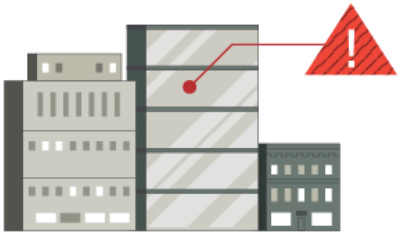
Medical Identity Theft and Fraud *(Cont.)*

Healthcare Fraud Detection and Remediation

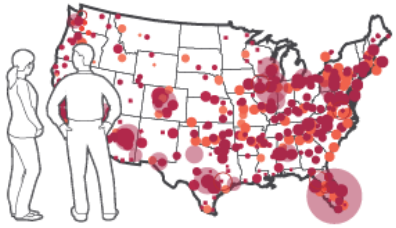
- If your investigation reveals medical identity theft, do you:
  - Notify the provider and the insured
  - Notify all entities and business associates
  - Consider the provider's role in the investigation
  - Consider law enforcement to conduct the investigation
  - Use technology to confirm medical transactions with patients before the transactions are processed

Medical Identity Theft and Fraud

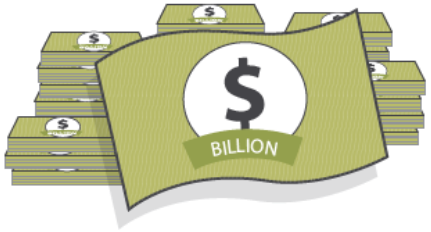
National Impact of Medical ID Theft



$20,000
average cost of medical ID theft incident



1.6 million
victims of medical ID theft — and growing



$70-234 billion
lost each year to healthcare fraud

Patient care and **health at risk** due to altered records

Specific Healthcare Industry Concerns and Challenges for Incident Response

- Theodore P. Augustinos
- Partner - Locke Lord LLP

Specific Healthcare Industry Concerns and Challenges for Incident Response

- Cyber Risks in the Healthcare Industry
  - Exposure of Information to Unauthorized Access or Acquisition
    - What Types of Information?
      - Personal Information (PI)
      - Protected Health Information (PHI)
        - » Created by CE, identifiable, relating to physical or mental health or medical condition or treatment
        - » Note: Any format – Often Not easily searched
  - What is Unauthorized Access?
    - Can present challenges due to definitions and exemptions, and the healthcare environment

Specific Healthcare Industry Concerns and Challenges for Incident Response *(Cont.)*

- Federal Push toward Electronic Data
  - Meaningful Use – mandate (ACA) and incentives (Medicare/Medicaid)
  - Makes Data more easily accessed and more vulnerable
- Sensitivity and Value of Data
- Need to have Data Accessible, often across systems and among entities
- Use of Vendors
- Cultural Issues

Specific Healthcare Industry Concerns and Challenges for Incident Response *(Cont.)*

- Legal and Regulatory Mandates
  - HIPAA/HITECH – HHS Privacy, Security, and Breach Notice Rules
  - State Requirements
    - More states are adding health and medical information to privacy, and breach notice requirements
    - New Jersey Encryption Requirements
      - Apply to health carriers
      - Others to follow. Expand beyond carriers?
  - High Risk of Individual and Systemic Harms
    - Healthcare is Critical Infrastructure under NIST
  - Compliance

Specific Healthcare Industry Concerns and Challenges for Incident Response *(Cont.)*

- Lack of Planning and Preparedness
  - Studies show having an Incident Response Plan reduces the cost of response
    - Over $12 per record, according to Ponemon study
  - Lack of a Plan/Lack of Preparedness
    - Delays the response
    - Jeopardizes effectiveness

Specific Healthcare Industry Concerns and Challenges for Incident Response *(Cont.)*

- Challenges in Forensics
  - Where's the Data?
    - Systems
    - Legacy Systems
    - Mobile Devices
    - Vendors
    - Unstructured Databases
  - What types of Data?
    - PI
    - PHI
    - Challenging Data Formats

Specific Healthcare Industry Concerns and Challenges for Incident Response *(Cont.)*

- Can we access information to show what happened?
  - Logging
    - » External
    - » Internal
  - Vendors and Cloud Services
- Challenges in Notification
  - Sensitivity of Services
  - Multi-Jurisdictional and International Incidents

Specific Healthcare Industry Concerns and Challenges for Incident Response *(Cont.)*

- Common Pitfalls
  - Lack of Investment of Time, Focus and Money
    - Insufficient technical capability
      - Encryption and other Security
      - Logging
      - Segregation and Restricted Access
      - Detection
      - Ineffective identification and management of risk profile
      - General lack of preparedness

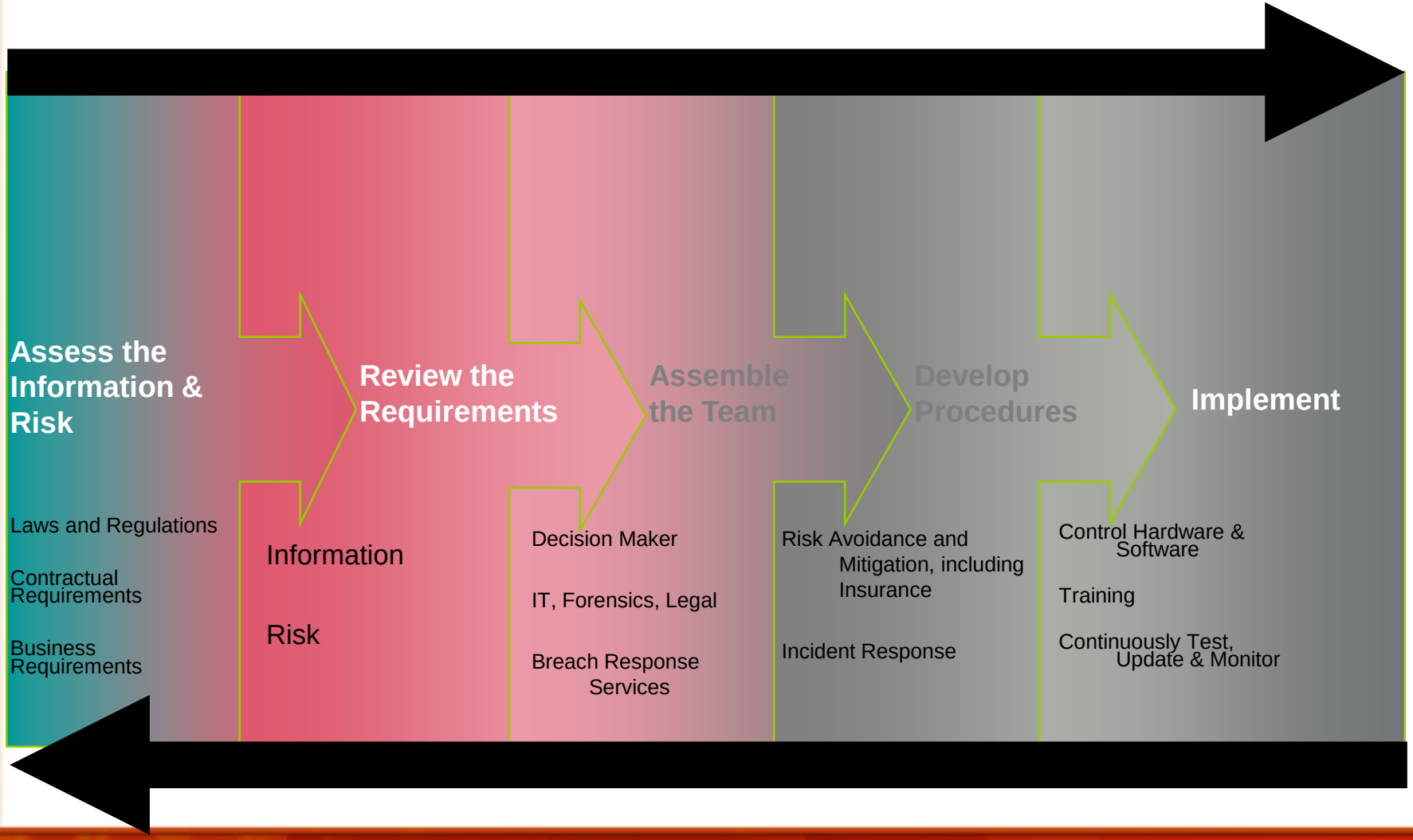
Specific Healthcare Industry Concerns and Challenges for Incident Response *(Cont.)*

- Ineffective Training
  - Increased vulnerability to Inadvertent or Malicious Incidents
  - Delayed or missed identification and escalation of incidents
- Lack of Understanding of Data and Systems
- Ineffective Vendor Management
- Data Minimization, Retention and Destruction
- Late Reporting

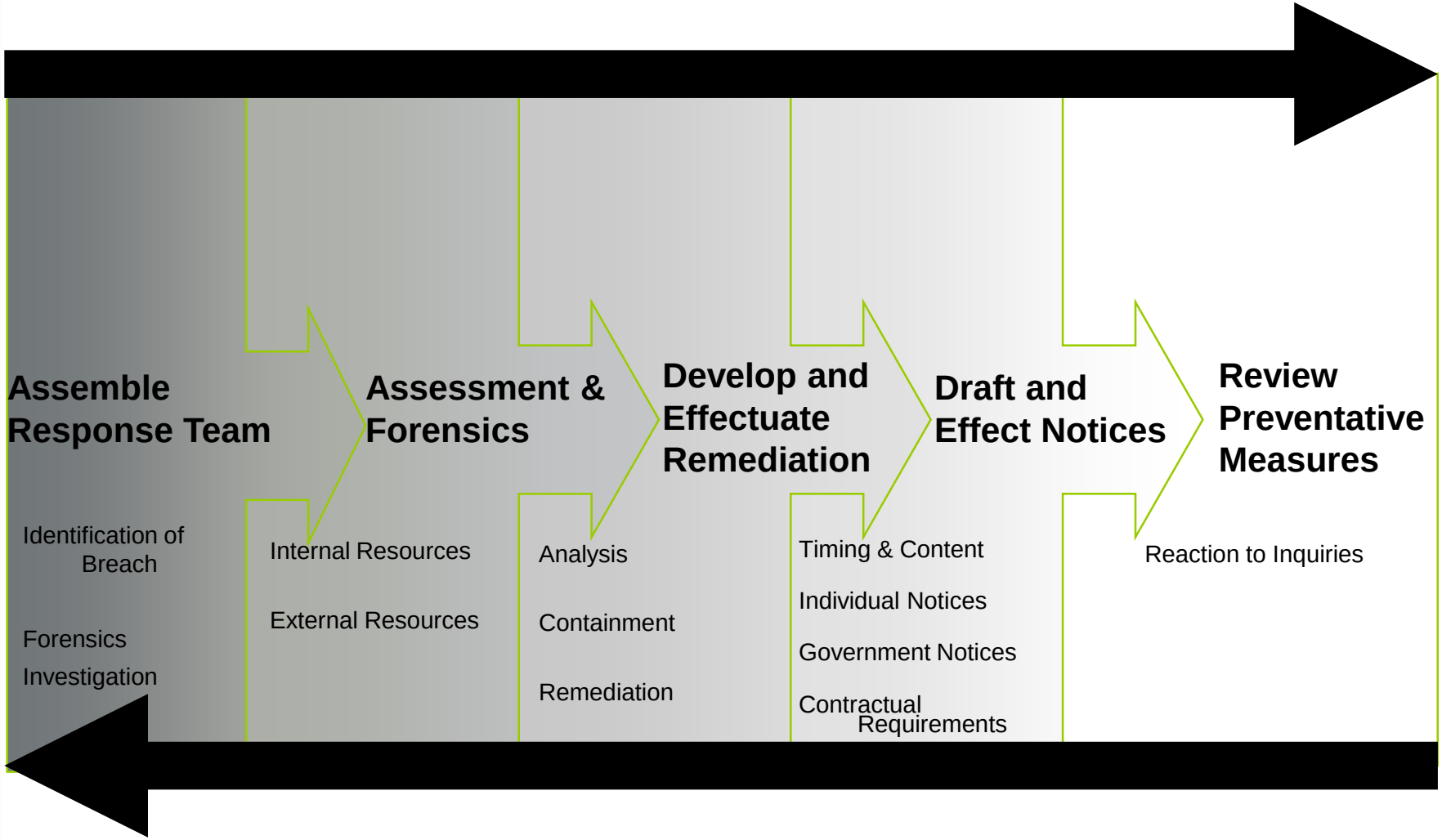
Specific Healthcare Industry Concerns and Challenges for Incident Response *(Cont.)*

- Premature Reporting
- Ineffective Messaging
- Ignoring the IRP

Avoiding Common Pitfalls in Healthcare Breaches: Preparedness



Avoiding Common Pitfalls in Healthcare Breaches *(cont.): Response*



The New Cyber Threat Environment and Corporate Data Governance Trends

- David S. Szabo
- Partner - Locke Lord LLP

The New Cyber Threat Environment and Corporate Data Governance Trends

MA HIPAA Breach Update

- Since enactment of HITECH in 2009 in Massachusetts:
  - 35 large HIPAA breaches in Massachusetts impacting 979,000 individuals, resulting in over $2.6 million in "resolution payments."
  - 6 laptop thefts/losses
  - 5 losses of paper
  - 17 theft cases
  - 8 hacking incidents

The New Cyber Threat Environment and Corporate Data Governance Trends *(Cont.)*

Nationwide HIPAA Enforcement Update

- Since 2008, nationwide, 23 OCR settlements/cases yielding nearly $26 million in fines or settlements.
- 2014 settlements include $1.75 million for a stolen laptop, $4.8 million for an unsecured server and $800,000 for records left in a doctor's driveway.
- OCR is increasingly focused on information security failures, such as lack of safeguards and failure to perform a risk analysis or violations of the breach notification rule, as opposed to privacy rule violations.
- What is the posture of your information security program?

The New Cyber Threat Environment and Corporate Data Governance Trends *(Cont.)*

MA AGO and OCABR Update

- According to OCABR 2013 Data Privacy Report, OCABR received 1,821 breach notices impacting over 1.2 million residents of the Commonwealth.
- The financial services sector accounted for 85% of the breaches. Healthcare accounted for 5% of reported breaches.
- AGO has settled at least seven data breach cases by consent orders filed in court, with fines ranging from $7,500 to $950,000.
- Most recently, Women & Infants Hospital paid $150,000 to the Mass AGO for a breach involving both PHI and Personal Information.

The New Cyber Threat Environment and Corporate Data Governance Trends *(Cont.)*

Dual Jurisdiction

- Beginning to see dual enforcement in breaches that involve both PHI and Personal Information.
  - Some Personal Information is also PHI, and some PHI is also Personal Information.
  - AGO has jurisdiction to enforce HIPAA rules, via HITECH amendments, even if no Personal Information is breached
  - The mechanics of “joint settlements” only now emerging, but many issues are unresolved.

The New Cyber Threat Environment and Corporate Data Governance Trends *(Cont.)*

- 2000: Introduction of HIPAA Privacy Rule: Privacy compliance was paramount. Penalties were modest, and reputation risk was the biggest concern.
- 2009: Stimulus package included funding for HIT and Meaningful Use. Security compliance attestation was needed to qualify for stimulus funds. Many providers attested routinely without regard to whether the attestation was accurate. HITECH enacted, including new penalties and breach reporting.
- 2013: Security incidents increase. Value of HIPAA settlements increases.
- 2014: First civil and criminal investigations of false MU Certifications occur.

The New Cyber Threat Environment and Corporate Data Governance Trends *(Cont.)*

- April, 2014: FBI Cyber Division Issues Private Industry Notification on Cyber Intrusions in Healthcare Systems and Medical Devices.
- According to one security consultant, “Stolen health credentials can go for $10 each, about 10 or 20 times the value of a U.S. credit card number.”
- DefCon 2014 Conference: Review of one large healthcare IDN revealed direct attack routes to networked infusion pumps, electronic health records, anesthesia systems, cardiology systems MRI, PACS and others. Risks include loss of data, integrity of data, and hostile attacks on patient care systems.
- October 2014, FDA issues updated guidance on cybersecurity for manufacturers of medical devices.

The New Cyber Threat Environment and Corporate Data Governance Trends *(Cont.)*

Lessons from the Big Box Breaches

- Breaches impacting customers of Big Box retailers are getting national attention, as numbers of impacted individuals are much larger than in typical health care breaches. Credit and debit card data are targeted.
- Target Breach: CEO resigned under pressure; CIO replaced; first CISO appointed; and activist investors targeted 7 of the 10 directors, although all 10 were re-elected to the Board.
- Shareholders have sued the board of directors for breach of fiduciary duty in connection with their oversight of corporate IT security.
- What is the role of your Board of Directors / Trustees in information security?

The New Cyber Threat Environment and Corporate Data Governance Trends *(Cont.)*

Governance and Information Security

- Since the financial crisis, public company boards face higher expectations to monitor management's efforts to deal with all sorts of risks to the corporation. Privacy and information security are one aspect of this increased emphasis on risk management.
- Public companies are expected to disclose cyber risks in annual and quarterly reports.
- In a 2014 speech, SEC Commissioner Luis Aguilar recommended that boards of directors of public companies include information security as one of the risk areas in which boards must supervise the activities of management.

The New Cyber Threat Environment and Corporate Data Governance Trends *(Cont.)*

Governance and Information Security

- He stated: "At a minimum, boards should have a clear understanding of who at the company has primary responsibility for cybersecurity risk oversight and for ensuring the adequacy of the company's cyber-risk management practices."
- He also suggested that corporate boards should review annual budgets for privacy and security programs, assign roles and responsibilities for privacy and security, and receive regular reports on breaches and IT risks.
- Where does information security fit into your governance structure?

The New Cyber Threat Environment and Corporate Data Governance Trends *(Cont.)*

OCR's initial questions

- Who in your organization is responsible for information security?
- When was a risk analysis most recently performed?
- Please send us a copy. . .

Thank You!

- Questions (and maybe Answers)