EPSTEIN BECKER GREEN

2010 HIPAA Security Environment

Managing Risk in the HITECH Act World

Prepared by

Mark Lutes, Epstein Becker & Green, PC
mlutes@ebglaw.com; 202.861.1824
Robert Hudock, Epstein Becker & Green, PC
rhudock@ebglaw.com; 202.861.1893; http://www.linkedin.com/in/rhudock

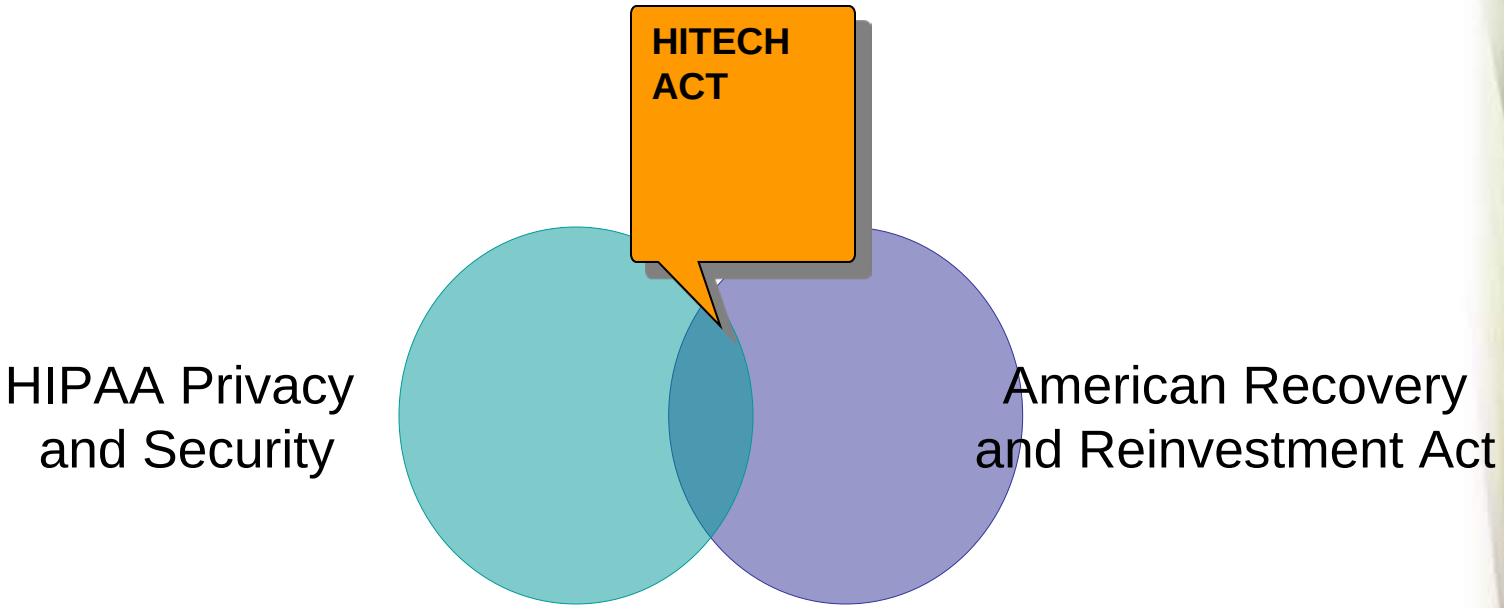
EBG

HIPAA

HIPAA
Health Insurance Portability and Accountability Act of 1996

- **Title I** — *Health Care Access, Portability, and Renewability*
- **Title II** — *Preventing Health Care Fraud and Abuse*; *Medical Liability Reform*; ***Administrative Simplification***
  - **Electronic Data Interchange**
    - **Transactions**
    - **Identifiers**
    - **Code Sets**
  - **Privacy**
  - **Security**
    - *Security Standards: General Rules*
    - *Administrative Safeguards*
    - *Technical Safeguards*
    - *Physical Safeguards*
    - *Organizational Requirements*
    - *Policies and Procedures and Documentation Requirements*
- **Title III** — *Tax-Related Health Provision*
- **Title IV** — *Group Health Plan Requirements*
- **Title V** — *Revenue Offsets*

Sorting it Out: HIPAA; ARRA; HITECH



Unrelated security issue: FTC “Red Flag” Rules around “creditors” having identity theft programs. ARRA incentives for meaningful use or rules for certifying EHRs not subject of this presentation.

Four Drivers of Increased Risk

- Direct application of HIPAA's Title II Security rule to Business Associates (BA's)**
- New Breach Notification Requirements under ARRA* (HITECH Act)*
  - Distinct from the Act's attempt to encourage adoption of Electronic Health Records ("EHR"s) by incentive payments for "meaningful use"
- New State Enforcement Authority Under HIPAA and Trend of State Legislated Private Rights of Action
- Government Audits

*Health Information Technology for Economic and Clinical Health (HITECH) Act, as part of the stimulus package (a.k.a. American Recovery and Reinvestment Act (ARRA) of 2009).

**A business associate is a third party that acts on behalf of a covered entity by performing a function or activity that HIPAA's Administrative Simplification rules regulate or that provides certain services (eg, legal or consulting services) that involve the use or disclosure of individually identifiable health information otherwise known as protected health information ("PHI").

Other HITECH HIPAA Impacts

- Extension of Key Security Provisions to Business Associates
  - Direct exposure to HIPAA civil and criminal penalties
- Penalties increased and “willful neglect” standard now included
- HHS Secretary, based on recommendations from the GAO Comptroller, required to develop mechanism whereby harmed individuals may obtain a percentage of the penalties by February 17, 2012
- Tightening definition of “minimum necessary”
  - implication for access controls under Security Rule and will impact form of BA agreement
  - Secretary to issue guidance on minimum necessary standard by August 17, 2010

Application to ERISA Plans

- **Plans have always been HIPAA covered entities.**

- **This fact has been obscured because privacy program responsibilities have been borne by:**
  - **insurer (assuming no more than summary health information went back to the plan and employer did not see it) or**
  - **the administrative services only ("ASO") provider (in self-funded context)**

HITECH reaches ERISA plans

- However, no such carve out from plan responsibilities exists relative to HIPAA security rule. Plan administrators need to exercise their fiduciary duties relative to the administrative, physical and technical safeguards of participant and beneficiary data whether held by insurer or by administrative services only entities
- HITECH reporting requirements apply to ERISA plans for data breaches occurring at the plan or BA level (need to work out responsibilities and decision making with ASO vendor) and liabilities apply as well.

Breach Notification under ARRA

EPSTEIN BECKER GREEN

- HITECH breach notice rule: was effective 9/23/09, fed enforcement deferred to 2/17/10
- Covered entity must notify individuals without unreasonable delay when there is a breach of individual's unsecured PHI and provide notice to the Secretary and, if affecting more than 500, the local media.
- BAs notify the Covered Entity (CE).
- Notice to include description of event, types of PHI disclosed, steps to take to protect, what the CE is doing to mitigate and prevent other occurences, and contact instructions.
- May be a game changer because: reporting exposes CEs and BAs to government investigation with new (more motivated?) "cops on the beat" and makes CEs and BAs adverse relative to consequences of reporting (adverse PR, notification costs, credit monitoring costs and other remediation)

EBG

Reporting Standard

- Statute: "unauthorized acquisition, use or disclosure…which compromises the security, privacy or integrity (of PHI)"
  - Exceptions where inadvertent disclosure to or by workforce, BA or organized health care arrangement participant
- Regulation: does the breach comprise the security or privacy of the PHI and "pose a significant risk of financial reputational, or other harm to the individual"

Breach Risk Assessment Factors

- OMB Memorandum suggests consideration of:
  - Nature of data elements breached;
  - Likelihood that the information is accessible and usable;
  - Likelihood the breach may lead to harm;
  - Ability of the entity to mitigate the risk of harm.
- Opportunity for forensic determination that privacy was not actually harmed
  - Controversial, Hill criticism, will HHS change?
- ***Consider in your incident response plan who will make these determinations, how you will combine IT and legal views and how you maintain privilege for your deliberations***

BA Agreement-Breach reporting provisions

Issues Include

- Timing of reporting
- What to report: "can BA make determination of no reasonable likelihood of information being retained?" What if BA disagrees with CE's conclusion?
- Overlap with "incident" reporting?
- For self-funded CEs, who reports?
- CEs seek indemnification (what damages?)
- BAs seek limitation on damages
- Information to be provided in report
- New attention to audits (routine or incident driven)

Examples of other BAA provisions now in play

- Business Associates required to notify the Covered Entity of breaches it discovers (its own or CE's), termination provisions now running both ways
- HHS Secretary is to provide **Annual** guidance regarding appropriate technical safeguards—how to accommodate
- Minimum necessary guidance coming from Secretary (BA to agree to sight unseen?)

STATE REPORTING REQUIREMENTS

Since 2003…

California 1st state to create data breach law in 2003

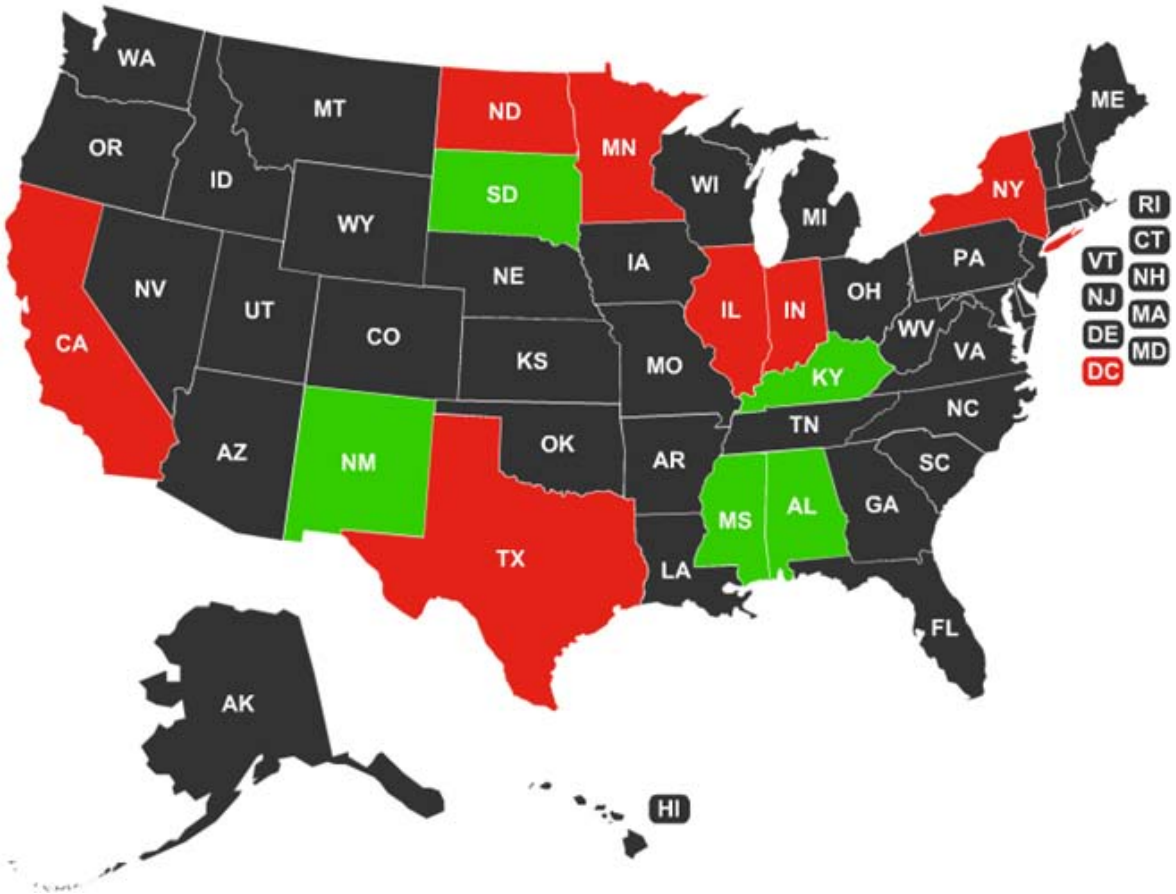
- ChoicePoint breach draws country's attention
- In less than 5 years, 44 additional states adopt breach laws

- Currently only Alabama, Kentucky, Mississippi, New Mexico, and South Dakota do not have statutes specifically addressing data security incidents

State Law Basics

- Notification requirement based on residence of affected consumers/patients, not the company
- States differ on requiring notice if based solely on acquisition of data or if harm from acquisition is reasonably likely
- A limited number of states specifically protect medical Information; expected to grow.
- Many states require pre-breach preventative procedures

Available at http://law2point0.com/wordpress/2009/09/15/50-state-security-breach-notice-law/



Red – Acquisition Based

Black – Risk Based

Green -- None

State Security Breach Notification Regulations

State Law Differences

- While many states have similar laws, key differences can significantly impact response strategies
  - Reporting to AG, civil penalties, private rights of action
  - Personal Information - the definition of "personal information" protected by statute can vary significantly
  - How and when must you report

Security Breach Statute Framework

Personal Information

- first name or initial and last name of an individual
- driver's license number
- Social Security number
- credit card or debit card number
- medical information or health insurance information

Statutory Notice Requirement

- Affected Individuals
- State Agencies
- Credit Reporting Agencies

Trigger

- Acquisition Based
- Risk Based
- Good Faith Acquisition Exception

Encryption

- Encryption is not defined and may mean a simple password.
- 128-bit or higher algorithmic encryption

Credit Freeze

- credit reporting agencies cannot release the frozen credit report without the consumer's express authorization.
- Security Alert Alternative

PREVENTION & RESPONSE

Prevention

Easily implemented procedures can greatly reduce the likelihood and cost of breaches:

- Cost of Notice- currently estimated at $214 per personal information account lost
- Expense for 18 months of credit monitoring
- Cost to Consumers
- Internal Diversion of Resources
- Reputational Cost

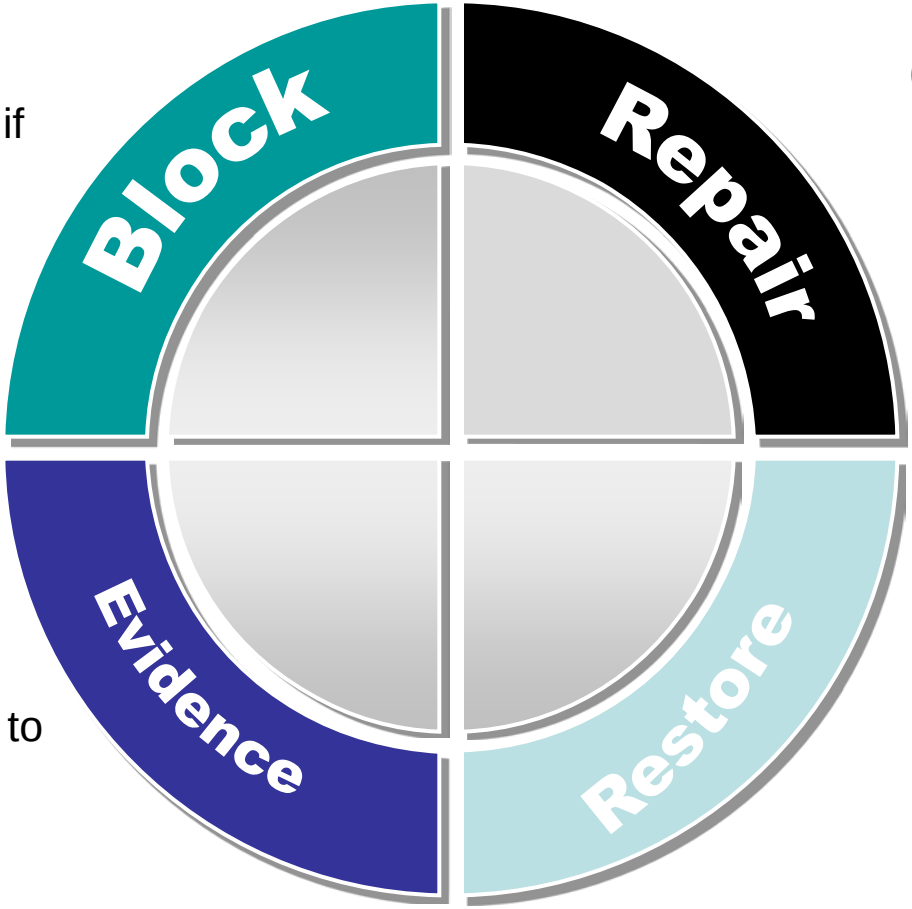
Common Sense Considerations

- Recent data breach research by GAO estimates that 87% of breaches could have been avoided if reasonable security measures had been in place at the time of the incident
- 59% of breaches occurred in companies that had security policies and procedures established but which were not actually implemented

Security Incident Response Policy

Written Incident Response Policy Is Essential

(1) Block or prevent escalation of the attack, if possible. Potentially disconnect the machine from the network.

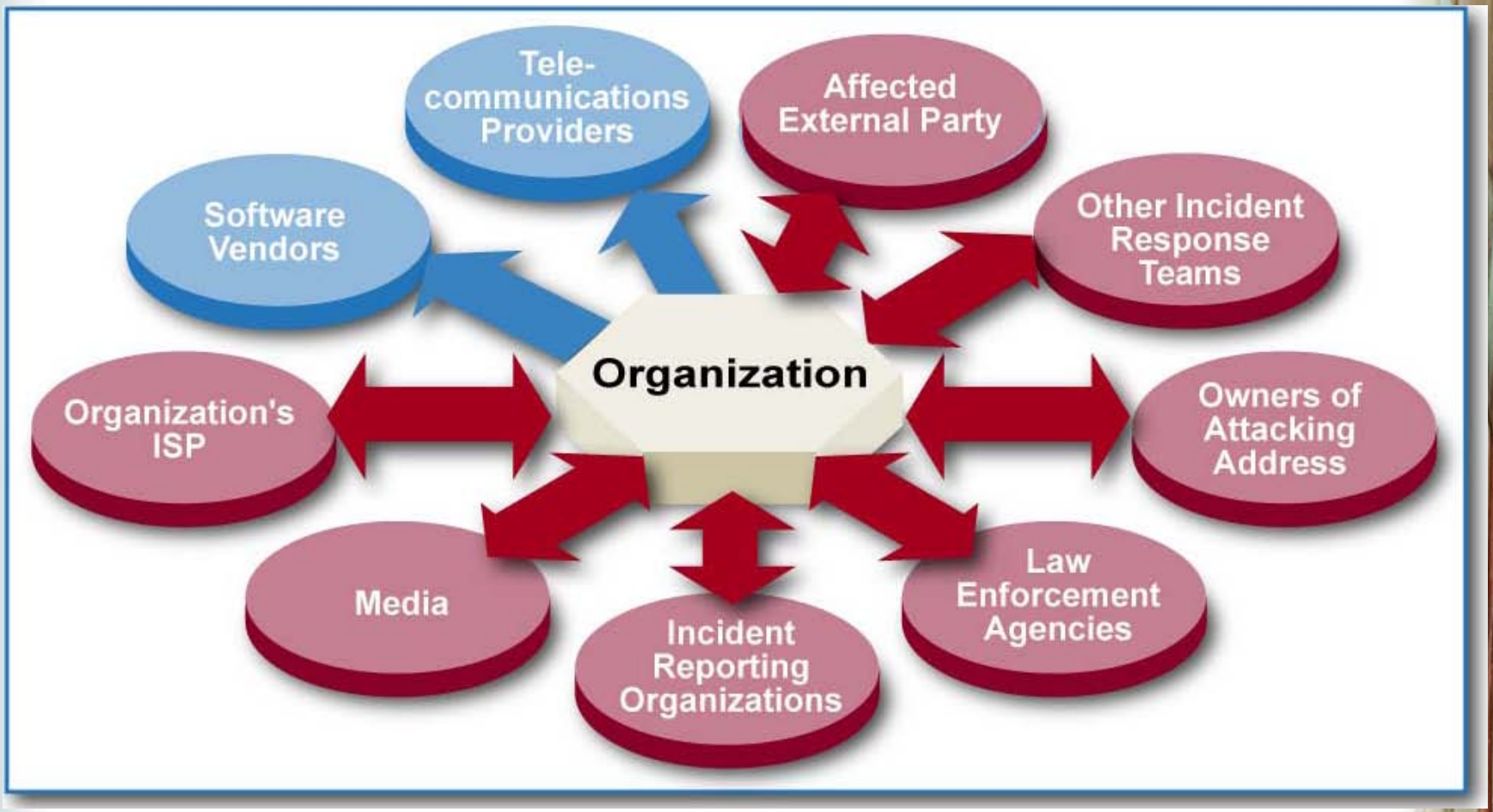


(2) Repair the resulting damage, if possible, without disrupting evidence.

(4) Preserve evidence, where appropriate. Try to determine extent of the exposure.

(3) Restore service to its former level, if possible.

Key Players in a Security Incident Response



Incident Response Preparedness

- Create an incident response policy
- Establish an incident response team/task force integrating legal and IT expertise
- Develop incident response analysis and reporting procedures that preserve privilege where appropriate
- Establish guidelines for communicating with external parties
- Establish and maintain accurate notification mechanisms. Draft an incident response notice in advance
- Develop written guidelines for prioritizing incidents
- Develop a detection, collection and analysis strategy*
- Focus on internal monitoring. Breaches, either malicious or accidental, by internal employees often tend to involve more records overall than do instances of external hacking

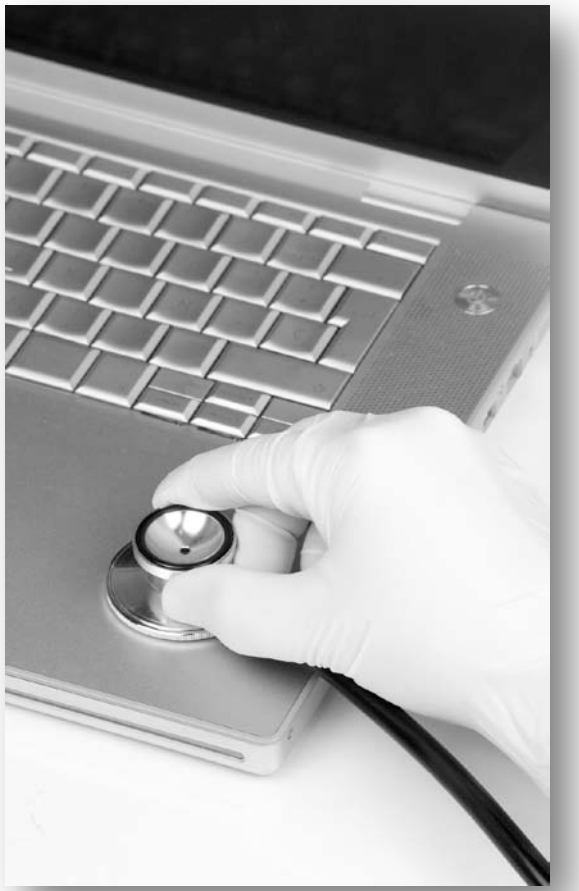
*Bowen, P., Hash, J, Wilson, M. "Information Security Handbook: A Guide for Managers." National Institute of Standards and Technology. U.S. Department of Commerce. 2006

Signs of an Ongoing Security Breach

- Network intrusion detector alerts of a buffer overflow in network service;
- Antivirus software detects a host is infected with a worm;
- Web server or database server crashes;
- Users complain of slow access to the Internet;
- Filename with unusual characters;
- Failed login attempts from an unfamiliar remote system;
- Large number of bounced e-mails with suspicious content; and
- Unusual deviation from typical network traffic flows

Typical Areas Needing Work

- Portable Media
  - Laptops, backup tapes, data shipping
- Network Vulnerabilities
  - IP addresses blocked, data transmission safeguards
  - Patching of client-side systems
- Written Incident Response Procedures



How will reporting risk be mitigated?

Reduce the amount of "unsecured PHI"

- For data at rest, electronic data that has been encrypted consistent with (NIST) Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*;
- For data in motion, electronic data encrypted with the requirements of Federal Information Processing Standards (FIPS) 140-2;
- For data on media, the paper, film, or other hard copy media has been shredded or destroyed such that the PHI cannot be read or otherwise reconstructed or the electronic media has been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitization*.
- How will CEs accomplish? Will they push down requirements to BAs?

.

Incident Rich Environment—experience this year alone

- E.g., payor in Tennessee has 57 unencrypted hard drives stolen from training facility implicating half million customers in 32 states
- Attorney General in Alaska settles with PriceWaterhouseCoopers over breach involving 77K retiree system participants
- Attorney General of CT files complaint against several health plans alleging HIPAA violations under HITECH Act authority including late notice, ineffective policies to protect PHI, failure to train and seeking injunctive relief and damages under HIPAA and state law (5K per incident)

Enforcement War Story

- On July 16, 2008, a health system entered into a resolution agreement with OCR whereby it agreed to pay $100,000 and implement a detailed Corrective Action Plan (CAP) to settle complaint stemming from its loss of unencrypted backup media and laptops in 2005 and 2006
- The CAP requires:
  - Revising policies and procedures regarding physical and technical safeguards (e.g., encryption) governing off-site transport and storage of electronic media containing patient information, subject to HHS approval;
  - Training workforce members on the safeguards;
  - Conducting audits and site visits of facilities; and
  - Submitting compliance reports to HHS for a period of three years.

* Pre-ARRA penalty caps kept settlement low, starting place for Office of Civil Rights negotiations will be higher in future

CVS Pharmacy

- January 16, 2009, CVS accepted $2,250,000 penalty and Corrective Action Plan (CAP) to settle complaint stemming from its practice of disposing of old prescriptions and prescription bottles
- The CAP requires:
  - Revising and distributing its policies and procedures regarding disposal of protected health information;
  - Sanctioning workers that do not follow the policies and procedures;
  - Training workforce members on these new requirements;
  - Conducting internal monitoring;
  - Engaging a qualified, independent third-party assessor to conduct assessments of CVS compliance with the requirements of the CAP and render reports to HHS;
  - New internal reporting procedures requiring workers to report all violations of these new privacy policies and procedures; and
  - Submitting compliance reports to HHS for a period of three years.
- Subsequently, OCR issued PHI Disposal FAQs

Are You Ready for an Audit?

- OCR work plan calls for audits and HITECH requires them
- Notice of breach will trigger audit
- Customers may negotiate for audit right in BA agreement or require them before contracting
- Who will be interviewed?
  - President, CEO, and Directors
  - HIPAA Compliance Officer
  - Lead Systems Manager or Director
  - Systems Security Officer
  - Disaster Recovery Specialist
  - Person in charge of data backup
  - Facility Access Control Coordinator
  - Human Resources Representative
  - Director of Training
  - Incident Response Team Leader

Documents Likely to be Requested During an Audit

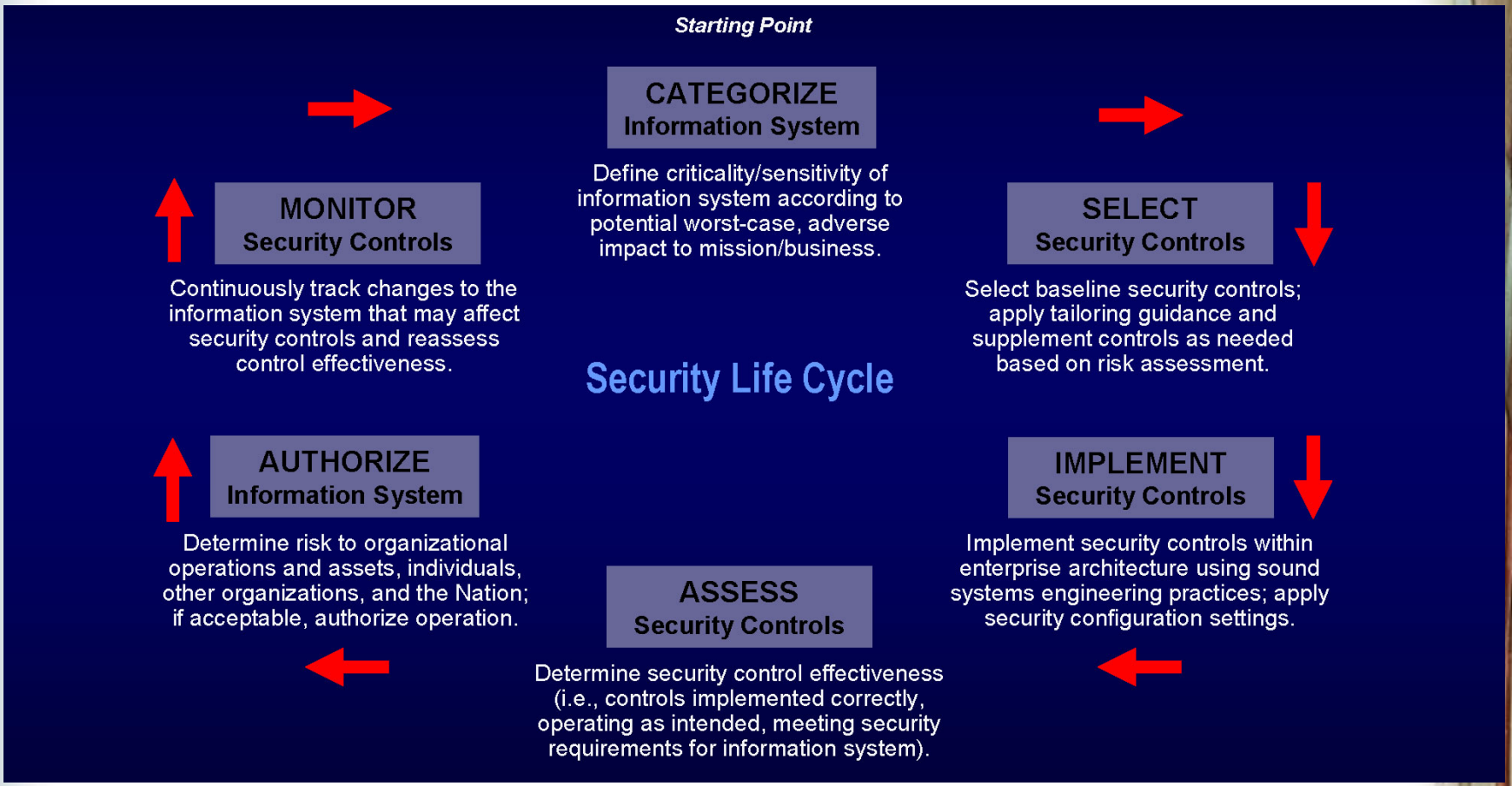
- Entity-wide security plan
- Most recent risk analysis
- Risk management plan
- Security violation monitoring reports
- Vulnerability scanning plans
  - Results from most recent scan
- Network penetration testing policy and procedure
  - Results from most recent network penetration test
- List of all user accounts with access to systems which store, transmit, or access ePHI (for active and terminated employees)
- Configuration standards to include patch management for systems which store, transmit, or access ePHI
- Organizational chart to include staff members responsible for general HIPAA compliance to include the protection of ePHI
- Examples of training courses or communications delivered to staff members to ensure awareness and understanding of ePHI policies and procedures
- Policies and procedures governing the use of virus protection software
- Disaster recovery plan
- Data backup procedures
- Analysis of information systems, applications, and data groups according to their criticality and sensitivity
- Inventory of all information systems to include network diagrams listing hardware and software used to store, transmit, or maintain ePHI
- List of all Primary Domain Controllers (PDC) and servers
- Inventory log recording the owner and movement of media and devices that contain ePHI

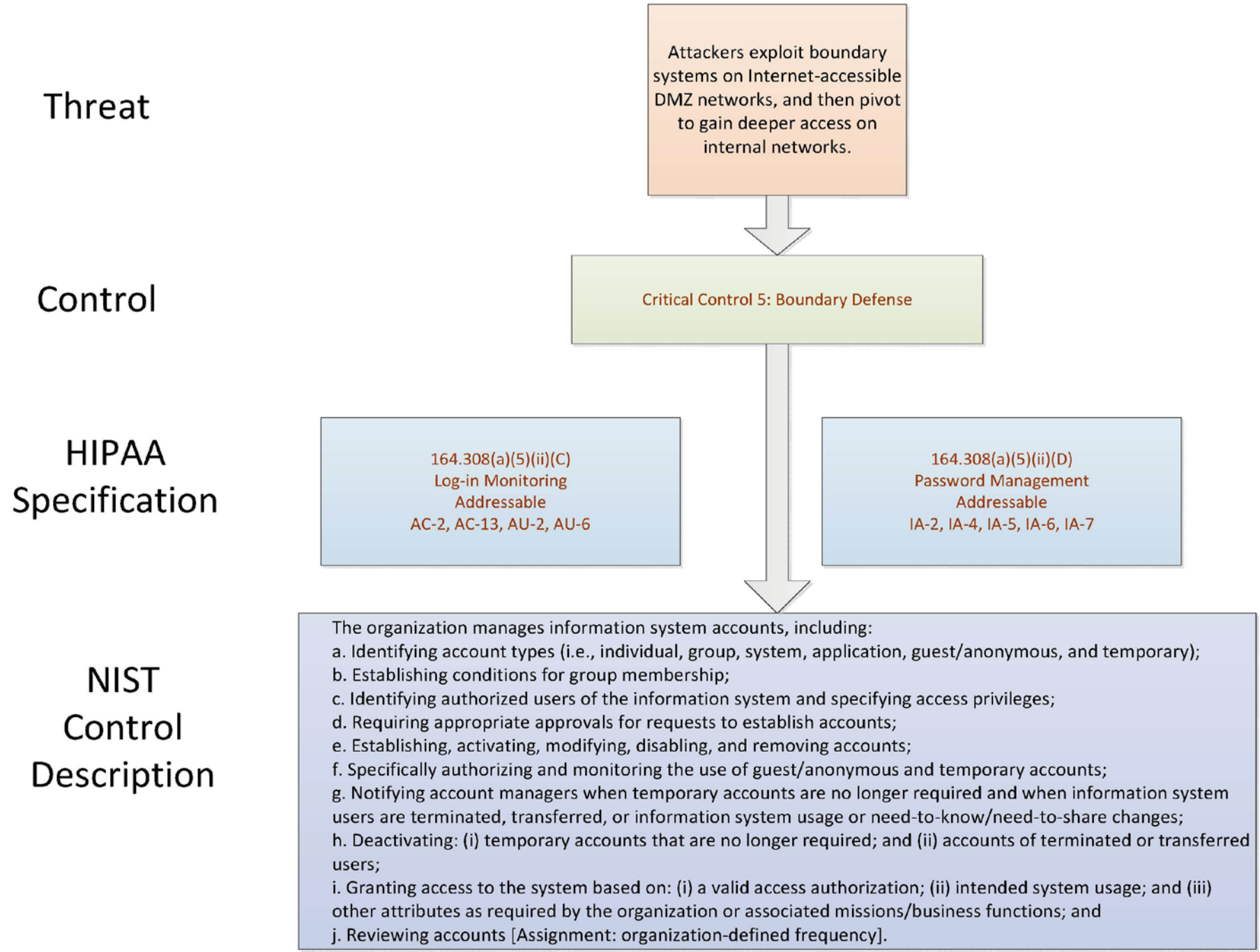
Specific Policies and Procedures Requested During a Security Audit*

- HHS Officials policies request includes:
  - Access Control Policy
  - Business Continuity Policy
  - Risk Analysis Policy
  - Compliance Policy
  - Data Transmission Policy
  - Security Incident Tracking Policy
  - Information System Monitoring Policy
  - Physical and Environmental Security Policy
  - Computer Use Policy
  - Wireless Network Security Policy
  - Firewalls, routers and switches
  - Information Systems Management Policy
  - Data Encryption Policy
  - Data Sanitization Policy

* OIG was interested in all these at Piedmont Healthcare

Security Life Cycle





Backbone of Effective Compliance Program

1. Periodic Assessment of Risk
2. Committee Prioritizes Issues
3. Committee Approves Work Plan
4. Audit Results
5. Report to Board

Committee minutes and other program documents need to reflect the above

Mark Lutes, Esq.
mlutes@ebglaw.com
Robert Hudock, Esq. CISSP
rhudock@ebglaw.com
Epstein Becker and Green, PC
1227 25th Street, Suite 700
Washington, DC 20037
(202) 861-0900
Blog: http://www.law2point0.com/chubb.pdf