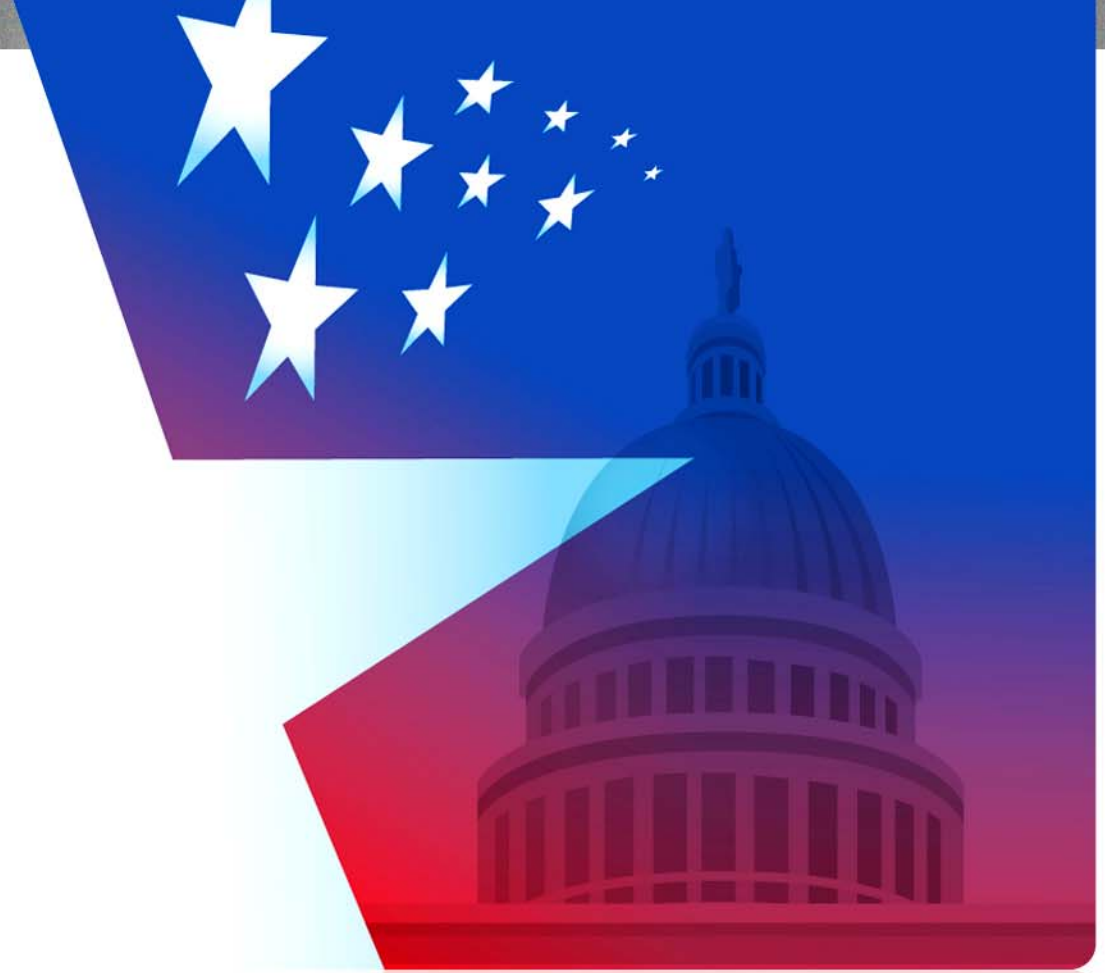


HIT The Ground Running: Risk Management Strategies to Jump Start Your Breach Compliance Program

Sharon R. Klein, Esq.
Pepper Hamilton LLP
kleins@pepperlaw.com

Carol Selvey MHSA, CPHIMS, FHIMSS
Associate Vice President,
Business Development
Iatric Systems, Inc.
carol.selvey@iatric.com

Pepper Hamilton LLP
Attorneys at Law

IATRIC systems

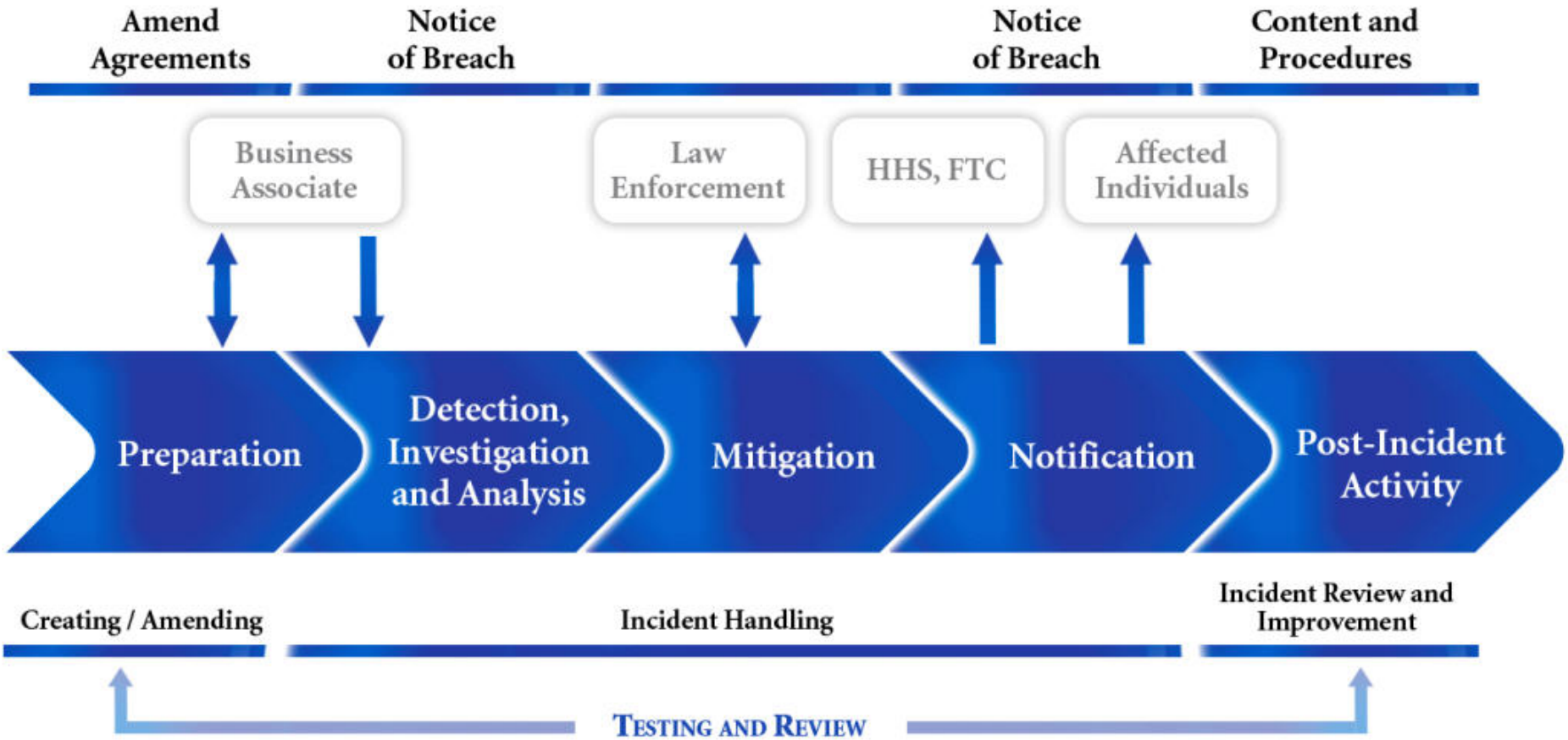
Background of HITECH Breach Notification

- 2-17-09 – Obama signs American Recovery and Reinvestment Act (ARRA)
- ARRA enhances privacy/security of Protected Health Information (PHI)
- 8-19-09 – HHS issues – final breach notification rule
- 9-23-09 – Compliance Date

Five Steps to Security Breach Response

1. Preparation (anticipating problems and potential litigation)
2. Detection, Investigation and Analysis (attorney client privilege)
3. Mitigation (applying best practices)
4. Notification (HHS final rules)
5. Post Incident Activity (evaluation and improvement).

Incident Response and Notification



Pepper Hamilton LLP
Attorneys at Law

IATRIC systems

Be Prepared

- Know the Laws/Regulations and Track Changes
  - Hundreds of laws and regulations in the US alone
  - Harmonize State and Federal laws
  - Organize Incident Response Team
  - Prepare Compliance Plan
  - Update business associate agreements so breach notice is promptly provided to CE

Detection, Investigation, Analysis

- Detection
  - Consider improving detection with network-based and host-based intrusion detection and prevention systems (IDPS), antivirus software and log analyzers
  - Internal human reporting mechanisms and provide training

- Procedures for reporting detected information security events and weaknesses to employees, contractors, and third-party vendors, including
  - Methods to promote effective and timely incident reporting and communication
  - Formal contact designation
  - Methods to ensure that incident escalation and response procedures are invoked and exercised
  - Mitigation methodologies

Detection, Investigation, Analysis

- Commence Investigation as soon as possible after the occurrence of an information security incident or event
  - Using audit trails, identify and analyze the causes of the information security incident, consider
    - external forensics support
    - possible communications with law enforcement
- Analyze to determine if a breach occurred, considering
  - If unsecured PHI involved
  - Probability of Harm (Risk Assessment)
  - Violation of the Privacy Rule
  - Individuals affected
    - how many
    - which states
- Analyze if other laws are applicable

Not a Breach if Privacy and Security of PHI not Compromised

- Security and Privacy Not Compromised if:
  - PHI Not Involved
  - PHI is "Secured"
  - There is No Risk of Harm

Not a Breach if PHI not Involved

- PHI is not involved if:
  - Health information that is the de-identified in accordance with 45 C.F.R. § 164.514(b)
  - Credit card information, account information and no health information
  - Categories of individually identifiable health information excluded from the definition of PHI, including:
    - Employment records held by a covered entity in its role as an employer
    - Certain student records
- Note: Consider whether other notification laws apply

Not a Breach if PHI is Secure

- There is no compromise to privacy and security PHI if PHI is "Secure"
  - Secure PHI is PHI that is rendered unusable, unreadable or indecipherable to an unauthorized individual
  - Guidance on making PHI Secure was provided by HHS on April 17, 2009 and further clarified by the comments in the Interim Final Rule
- By definition, a Breach only involves unsecured PHI

Securing PHI

- Encryption
  - the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key 45 C.F.R. § 164.305
    - And the confidential process or key that enables decryption has not been breached
- Destruction:
  - Rendering PHI unusable, unreadable or indecipherable by total destruction

Valid Encryption Processes

- Data at Rest
  - NIST Special Publication (SP) 800-111 *Guide to Storage Encryption Technologies for End-User Devices*
- Data in Motion
  - SP 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*
  - SP 800-77, Guide to IPsec VPNs
  - SP 800-113, Guide to SSL VPNs, or
  - Other Federal Information Processing (FIPS) 140-2 validated standards
- Data Disposed
  - NIST Special Publication 800–88, *Guidelines for Media Sanitization*

Not a Breach if There is no Harm

- A compromise of the security and privacy of the PHI must pose a significant risk of financial, reputational or other harm to the individual
  - A risk assessment must be conducted to determine if harm exists

Risk Assessment Factors

- With regard to impermissible disclosures:
  - Were the recipients obligated to protect privacy and security of the information?
    - GLBA, HIPAA, FISMA, Corporate Policies?
  - Can the impact of the disclosure be mitigated?
    - Did CE or BA obtain a NDA or other satisfactory assurances that the information would not be disclosed further?
  - Was it returned before an improper use?
    - e.g., laptop returned and forensics investigation reveals improper use
  - What is the type and amount of the disclosure?
    - Financial, personal, sexual, identifies disease sates or treatment information that embarrasses or may lead to identity theft or employment discrimination, etc.
- The Comments refers readers to OMB Memorandum M-07-16 for further guidance on risk assessment factors

Mitigation

- Legal Risk Mitigation Strategies
  - Analyze best policies, procedures and practices
    - Update frequently so they work in practice
    - Audit or independent reviews
  - Clear identification of responsible employees/officers
  - Training of employees and third parties
  - Audit or oversight of parties handling or having access to your data
  - Involvement in appropriate associations

HHS Breach Notification Procedures

- "Without reasonable delay" 60 days after discovery of breach
  - 60 days commences when discovered by CE/BA
  - Notice may be delayed at request of law enforcement
- Individual Notice
  - Written Notice
    - Preferred method of communication
    - First-class mail or e-mail if requested
  - Telephone or other means – if there is urgency of imminent danger

HHS Breach Notification Procedures (cont'd)

- Substitute notice if 10 or more cannot be reached – website, print or media
- Use of Media Outlets in a state or jurisdiction is a required method if more than 500 residents of a state or region are affected
- Notice to HHS
  - Immediately if breach involves 500 individuals
  - Annual notice to HHS if fewer than 500 individuals

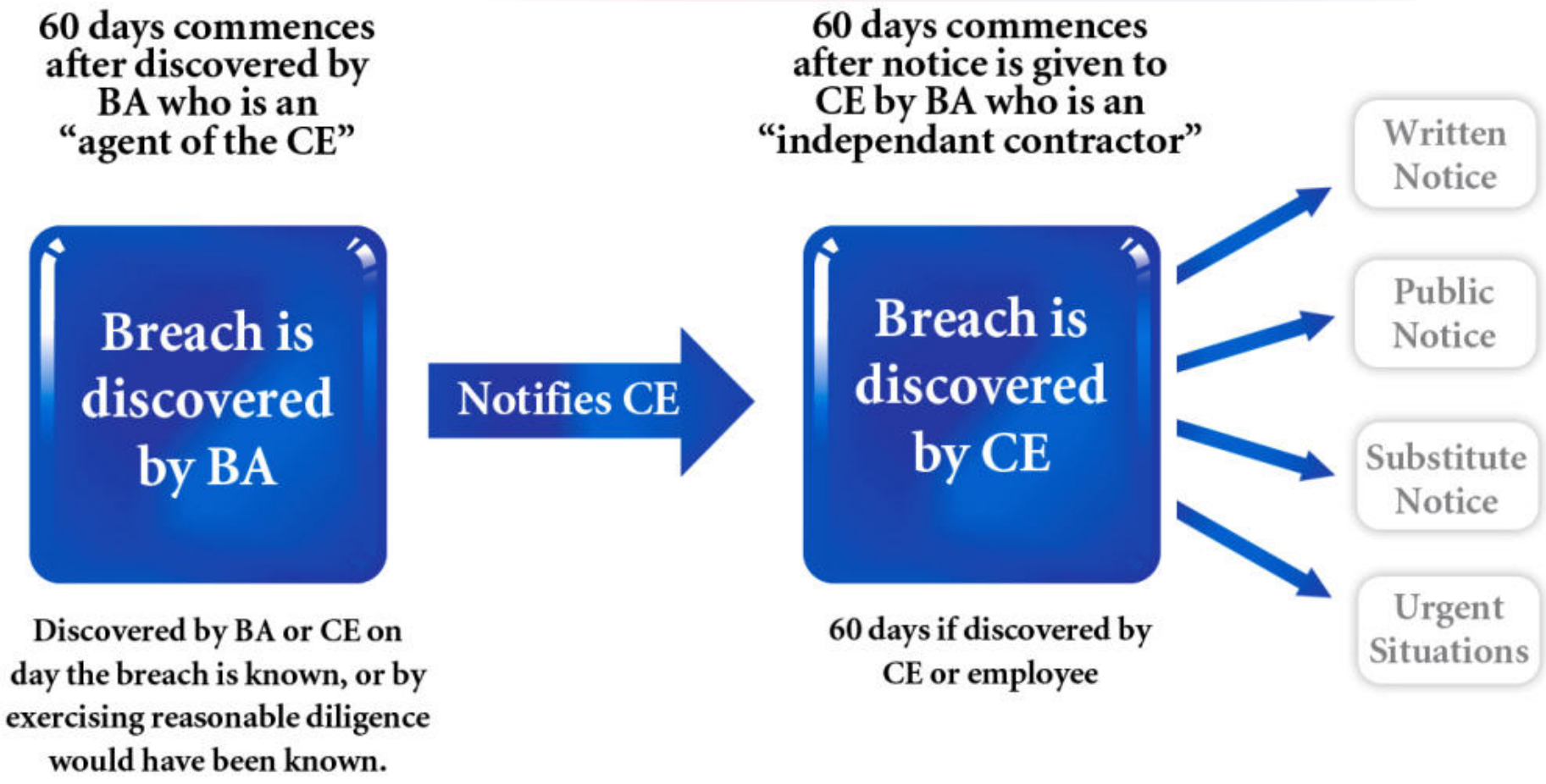
Notification for Breaches of PHI

- Applies to BAs and CEs that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured PHI
- A "breach of security" is an unauthorized *acquisition, access, use, or disclosure* of PHI in a manner not permitted by the Rule and which compromises the security and privacy of the PHI
- Content and timing
- Public/Private notification

HHS Breach Notification Content

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
- A description of the types of unsecured PHI that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code);
- The steps an individual should take to protect him/her self from potential harm resulting from the breach;
- A brief description of what the covered entity involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches; and
- Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, and e-mail address, Website, or postal address.

Imputed Knowledge and Agency Rule



Pepper Hamilton LLP
Attorneys at Law

IATRIC systems

Notification by a Business Associate

- A BA discovering the breach must notify the CE
  - Is "discovered" the day the breach is known, or by exercising reasonable would have been known
- To be provided without unreasonable delay and in no case later than 60 calendar days after discovery
- Content
  - Identification of each affected individual
  - Other information that the covered entity is required to provide in its notification to affected individuals

Post Incident Activity

- Evaluation loop (what worked/what did not work)
- Review and update HIPAA compliance plan
  - Awareness training of workforce
- Incorporate lessons learned into Incident Response and notification plan for unsecured PHI
- Consider Encryption and De-identification
- Continuous improvement

Thank You

Sharon R. Klein, Esq.
Partner
Pepper Hamilton LLP
Phone – (949) 567-3580
kleins@pepperlaw.com

Carol Selvey MHSA, CPHIMS, FHIMSS
Associate Vice President,
Business Development
Iatric Systems, Inc.
Phone/Fax – (978) 805-3451
carol.selvey@iatric.com

Pepper Hamilton LLP
Attorneys at Law

IATRIC systems