



# Elements of a Swift (and Effective) Response to a HIPAA Security Breach

---

**Susan E. Ziel, RN BSN MPH JD**  
**Krieg DeVault LLP**  
**Past President, The American Association of**  
**Nurse Attorneys**



# Disclaimer

---

- **The information contained in this presentation has been prepared with the understanding that the author is not engaged in rendering legal, financial, medical or other professional advice.**



# Applicable Requirements

---

- **HIPAA Privacy and Security Rules**
- **State Laws Requiring Notice of Security Breaches Involving Personal Information**
- **Laws Protecting Other Information**
- **Identity Theft and Crediting Reporting Laws (ITADA, FCRA, FACTA)**
- **Industry Standards (ISO, NIST, SAS 70)**
- **Other**



# Typical Scenarios

---

- **Employee sold terminally ill patient IDs resulting in fraudulent mortgages**
- **Contractor stole patient IDs and obtained fraudulent credit**
- **Hospital ER “imposter” collected and sold patient IDs**
- **Consultant downloaded PHI to “jump drive” which was lost and never retrieved**



# More Typical Scenarios

---

- Employee had laptop stolen from her unlocked car
- Consultant pocket PC containing client file information left behind in restaurant
- “Loaded” CDs inadvertently thrown into trash
- Hacker accesses data through Internet website
- Malicious software (virus) takes down electronic information system
- Unencrypted PHI emailed to wrong address

# PHI Protected by HIPAA



---

- Any health or demographic information collected from patient
- That is created or received by covered entity
- Which relates to an individual's past, present or future physical or mental health of patient and related treatment and payment functions
- For which there is a reasonable basis to believe the information can be used to identify the patient



# PI Protected by State Law [e.g., IC 24-4.9-2]

---

- **Unencrypted SSN (or)**
- **Name plus one or more of the following unencrypted or unredacted data:**
  - **Drivers license number**
  - **State identification card number**
  - **Credit card number**
  - **Financial account or debit card number plus security code, password or access code**



# PHI vs. PI

---

- **HIPAA**

- **Covered Entity**
- **Security Incident**
- **Electronic Media**
- **Protected Health Information**
- **Safeguards**
- **Obligations**

- **State Security Breach Laws**

- **Data Base Owner**
- **Security Breach**
- **Electronic Media**
- **Personal Information**
- **Safeguards**
- **Obligations**



# Security Incident

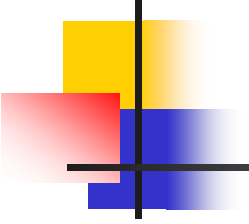
## HIPAA

---

- Any attempted or successful (and)
- Unauthorized access, use, disclosure, modification or destruction (of)
- PHI, system operations, electronic media or other components of an information system containing PHI

# Security Breach

[e.g., IC 24-4.9-2-2]

- 
- **Unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of Personal Information maintained by a person, but excludes:**
    - Good faith acquisition by authorized person for authorized purposes
    - Unauthorized acquisition of portable electronic device that is password protected
  - **Computerized data includes data transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in a computerized format**



# Disclosure of Security Breach [e.g., IC 24-4.9-3-1] if ...

---

- Learns that PI was or may have been acquired by unauthorized person and
- Knows, should know or should have known that the unauthorized acquisition has resulted in or could result in identity deception, identity theft or fraud.



# Important Safeguards

---

- **Laws and regulations, institutional policy**
- **Access and crowd control**
- **Marking and labeling documents**
- **Engaging counsel and asserting privilege at appropriate time**
- **BAAs and non-disclosure agreements**
- **Information and electronic media management**



# Laws, Regulations and Institutional Policy

---

- **(Most stringent) laws and regulations**
  - **Medicare conditions of participation**
  - **State licensure**
  - **HIPAA and other privacy/security laws**
- **(Adopted) institutional policy**
  - **Reported HIPAA security incident**
  - **Confirmed HIPAA security breach**



# Does Your HIPAA Policy Define All of These Terms?

---

- Access or Acquisition
- Availability
- Confidentiality
- Disclosure
- Electronic Media
- Encryption
- Identity Deception or Theft
- Integrity
- Personal Information
- Privacy
- Privacy Incident
- Protected Health Information
- Redacted
- Security
- Security Incident
- Unauthorized Access or Acquisition



# Does Your HIPAA Policy Include These Provisions?

---

- How to report both HIPAA privacy and security incidents
- The members of the “rapid response” team
- How to implement contingency plan
- Essential steps to proper investigation
- Who decides whether
  - The incident qualified as an unauthorized access and
  - The unauthorized access has or could have resulted in identity deception or theft; fraud



# Does Your HIPAA Policy Address Sanctions?

---

- **Level 1: Careless Access to PHI**
- **Level 2: Intentional Access to PHI for Personal Reason or Gain**
- **Level 3: Intentional Access to PHI for Financial Gain or Malice**





# Access and Crowd Control

---

- Premises and workstations
- Keys and passwords
- Workforce, business associates and business visitors
- Mobile electronic media
- Communication in any form/medium
  - Face to face
  - Telephone, facsimile, email
  - Mobile electronic media



# Information and Electronic Media Management

---

- **Inventory and Mapping**
- **Back-up**
- **Fixed vs. mobile**
- **Transmission**
- **Storage**
- **Transfer and re-use**
- **Retirement and destruction**



# Investigational Materials Segregated and Labeled

---

- **Confirm applicable privilege**
- **Establish policy and procedure**
- **Separate investigational files**
- **Document footers claiming privilege**
  - **Prepared in anticipation of litigation or administrative proceeding**



# Engaging Counsel and Asserting Privilege Timely

---

- Segregate privileged communications
- Only counsel and essential persons present for privileged communications
- Clear counsel reporting relationship
- Clearly labeled and contains legal advice
- No third party disclosures
- Work product created with intent to remain confidential



# What If You Need to Engage an Expert?

---

- **Types of Experts and Advisors**
  - Public Relations
  - Forensic Specialists
  - Other
- **Engagement by Counsel**
  - Nature of Services
  - Establish Communication Rules
  - Don't Forget the BAA



# Identity Theft Protections

---

- Report incident to credit reporting agencies
- Annual credit reports
- Credit protection services
- Identity theft insurance
- Other



# Proper Use of Service Agreements and BAAs

---

- Parties
- Scope of services
- Scope of PHI access
- Safeguards required
- Reporting of inadvertent disclosures
- Indemnification
- Return or destruction of protected information
- Termination



# Does Your BAA Incorporate All of These Terms?

---

- **Comply With HIPAA and Other Laws Governing Privacy and Security of PHI and PI**
- **Institute Administrative, Physical and Technical Safeguards**
- **Protect Privacy of PHI and Security of EPHI**
- **Report Security Incidents**
- **Indemnify for Violations of HIPAA and Other Laws**





# Key Elements of an Effective (and Swift) Response Plan

---

- #1. Notify Your Key “Need to Know”  
Persons; Establish Phone  
Conference Schedule**
- #2. Set Mitigation Experts in Motion**
- #3. Notify Counsel and Engage  
Necessary Experts**



# Key Elements of an Effective (and Swift) Response Plan

---

**#4. Establish a Public Relations Plan**

**#5. Conduct and Document a  
Confidential Investigation Process**

**#6. Secure Evidence and Maintain  
Chain of Custody**



# Key Elements of an Effective (and Swift) Response Plan

---

**#7. Corrective Action Plan and  
Progress Reports**

**#8. Determine Notification  
Obligations**

**#9. HIPAA Accounting Obligations**



# Key Elements of an Effective (and Swift) Response Plan

---

**#10. Call Center Arrangements**

**#11. Institute Identity Theft  
Precautions, If Necessary**

**#12. Be Prepared to Respond To  
External Investigations**



# Resources

---

- [www.hhs.gov/ocr/hipaa/](http://www.hhs.gov/ocr/hipaa/) (OCR)
- [www.cms.hhs.gov/EducationMaterials/04\\_SecurityMaterials.asp#TopOfPage](http://www.cms.hhs.gov/EducationMaterials/04_SecurityMaterials.asp#TopOfPage) (CMS)
- [http://www.consumersunion.org/campaigns/Breach\\_laws\\_May05.pdf](http://www.consumersunion.org/campaigns/Breach_laws_May05.pdf) (State Laws)
- [http://csrc.nist.gov/itsec/guidance\\_WinXP.html](http://csrc.nist.gov/itsec/guidance_WinXP.html) (NIST)
- <http://www.consumer.gov/idtheft/> (FTC)
- [sziel@kdlegal.com](mailto:sziel@kdlegal.com) (Susan Ziel)