Who's Afraid Of A Big Bad Breach?:

Updates on HITECH and State Breach Notification and Security Requirements

Robin Campbell

HOOPS2010

Crowell & Moring LLP

Overview

- Identifying the laws that protect personal information and protected health information
- Understanding the basics of what they require
- How to prevent a breach
  - Assessing your business need for PI/PHI
  - Protecting PI/PHI with administrative, technical, and physical safeguards
- How to respond to a breach
  - Train employees to recognize an incident
  - Advertise reporting mechanisms
- Consequences of a Security Breach
- New Trends in State Law

Laws that Protect Personal Information

- Federal
  - HIPAA (CEs and BAs)
  - GLBA (includes insurers and their service providers)
  - FACTA (use of consumer reports/background checks)
- State
  - State Breach Notification Laws
    - Massachusetts regulations
    - Nevada encryption standards
  - State SSN laws
  - State mini-HIPAA laws
- Other: Marketing, Telemarketing, CANSPAM, PCI/DSS

HIPAA/HITECH Breach Notification

- Statutory definition of breach:
  - The unauthorized acquisition, access, use or disclosure of protected health information, which compromises the security, or privacy of such information…

Requires written notification to the individual without unreasonable delay but *no later than 60 days from discovery (same timeframe for CE to notify individual and BA to notify CE)*

Clock starts ticking when 1st workforce member or agent knew, or by exercising reasonable diligence would have known

Risk of Harm Standard

- HHS has determined that "compromises the security or privacy of the protected health information" means that the breach poses a "significant risk of financial, reputational, or other harm to the individual"
- Notification is only necessary if the breach poses a significant risk of harm
- CEs and BAs must document their risk assessment to demonstrate that notification was not required

Assessing the Risk

Factors to consider:

- To whom was the information disclosed?
- What steps were taken to mitigate the breach?
- What type of information was compromised?

Information Covered

"Unsecured protected health information"

- PHI as defined by HIPAA (paper or electronic)
- HHS provides specific encryption standards for data at rest and data in motion
- Paper documents can only be secured through shredding or destruction

Notifications Required

- Individual
  - Written via US mail
  - Substitute if there is insufficient contact info for 10 or more individuals
- If more than 500 residents of a state or jurisdiction are affected, must notify prominent media outlets in that state or jurisdiction
- If 500 or more individuals in total are notified, must notify HHS within 60 days
- If less than 500 individuals, HHS must be notified in an annual report

Notifications to HHS are posted on its website

Other Notification Requirements

- State AGs
- State regulators (DOI, Medicaid regulators, Consumer Protection Offices)
- CMS (Centers for Medicare and Medicaid Services) for Medicare Advantage Organizations and Part D Plan Sponsors

Implications of Regulator Involvement

- Some require notice before notifying individuals
- Some want to approve notice content

What to do…

- Plan regulator approval of content into your timing
- Prepare template forms that they can approve in advance if you deal with them often (e.g. CMS)
- Prepare for more stringent demands from regulators for consumer protections (e.g. credit monitoring, credit restoration, reimbursement, insurance, etc.)

States with Breach Laws

Alaska	Kansas	Ohio
Arizona	Louisiana	Oklahoma
Arkansas	Maine	Oregon
California	Maryland	Pennsylvania
Colorado	Massachusetts	Puerto Rico
Connecticut	Michigan	Rhode Island
Delaware	Mississippi	South Carolina
District of Columbia	Missouri	Tennessee
Florida	Minnesota	Texas
Georgia	Montana	Utah
Hawaii	Nebraska	Vermont
Idaho	Nevada	Virginia
Illinois	New Hampshire	Washington
Indiana	New Jersey	West Virginia
Iowa	New York	Wisconsin
	North Carolina	Wyoming
	North Dakota	

Requirements of State Laws

- Generally require written notification to individual in the event of a breach of security similar to HITECH
- Each state varies in:
  - the definition of what constitutes a breach
  - the definition of personal information (only a few include PHI)
  - inclusion of a risk of harm standard
  - content requirements for notice
  - authorities that must be notified
  - available penalties and private right of action

No Preemption

- HHS guidance implies that state breach laws will not be preempted—it is possible to comply with both HITECH and applicable state laws

Federal/State The Venn Diagram

- PHI versus PI
  - PHI without SSN would not be covered in most states
- Paper versus Electronic Data
- Risk of Harm versus None
  - Don't forget that if you make a determination that there is no risk of harm under HIPAA breach rules, you must still notify in CA, ND (DOB only), PR and TX which include PHI and have no risk of harm standard
- Federal content versus State
- 60 days versus Without Unreasonable Delay (or 45 days)
- Notice to HHS/FTC/CMS versus or in addition to State AGs, DOIs and other regulators

What to Do

- Assess the NEED for the data:
  - Ask whether the PHI/PI is needed to complete a particular task
  - Does the intended recipient need the data with individual identifiers?
- If the data is needed, LIMIT ACCESS to those who need to see it, store it, transfer it and dispose of it
- ENSURE that everyone with access is AWARE that the data includes PHI/PI and must be TREATED CONFIDENTIALLY (be specific about what that means, i.e. encryption, locked offices and drawers, no portable media, etc.)
- Train, Train, Train—Enforce, Enforce, Enforce

Prevention

- Reasonable and adequate security procedures (administrative, technical and physical)
- Contractual safeguards for transfer
- Effective and timely destruction methods and policies
- Limit access to personal data
- Require adequate security of third parties through contract and know your own contractual obligations as a vendor
  - Update existing vendor agreements
  - Specify minimum security requirements
  - Include a notification requirement for incidents
  - Provide for indemnification for breach costs
  - Know your own contractual obligations—confidentiality, security, timelines for notice of incidents, indemnification

Administrative, Technical & Physical Safeguards

- Administrative
  - Policies and Procedures
  - Incident Response Plan
- Technical
  - Main risks lie in portable media (disk, flash drives, portable drives, laptops) and unsecured transfers (email over Internet or use of wireless networks)
  - Encryption is industry standard for portable media—combined with policy that limits data to be downloaded to portable media
  - Encryption for transfer over email
- Physical
  - Clean desk policy
  - Locked office/window when PI/PHI in room
  - Keep confidential information in locked file cabinets
  - Lock out system on computer when not in use

How to Respond to Breach

- Secure the information/systems
- Conduct investigation
- Involve law enforcement as necessary
- Involve regulators/authorities as necessary
- Categorize data lost
- Document incident and response
- Be prepared with public statement (press release to media)
- Be consistent in statement, policy, practices
- Prepare for inquiries (policies, contracts, audits)
- Letters to individuals
- Letters/electronic submission to authorities (state AGs and others, HHS)
- Letters to CRAs
- Call Center FAQs/Call Script
- Document risk of harm assessment if not sending notification
- Vendor: Credit Monitoring, Notification

Enforcement

- Breach notification often leads to scrutiny of underlying privacy and security practices
- Greater penalties under HITECH
- HHS now has up to $1.5 million
- State AGs have $100 per violation, up to $25,000
- State AGs also have independent fines available under the state security breach laws or state unfair trade practices laws
- State DOIs have separate authority to enforce state insurance laws with different penalties
- Does not appear to be a limit on the number of state AGs that can bring enforcement under HIPAA for privacy and security rule violations

Consequences of a Breach

Enforcement Options:

- Penalties for failure to notify under the statutes (range from $0 to $750k for multiple violation)
- Injunctive relief
- Restitution
- Private right of action established by statute in many states
- Class action
- OCR complaint
- FTC penalties and oversight

Costs associated with notification:

- Direct
  - forensic experts
  - notification letters
  - credit monitoring
  - Insurance coverage
  - call centers
  - discounts on future products or services
- Indirect
  - responding to state/federal investigations and customers
  - lost customers

  Cost per record now over $250, expensive process, damage to reputation even more significant

  PUBLICITY, PUBLICITY, PUBLICITY — HHS posting on website, Some states also, Media notification required for larger breaches under HIPAA (500 individuals)

Massachusetts/Nevada Regulations

Massachusetts

Detailed Technical Requirements—"to the extent technically feasible" that include:

- Encryption of all transmitted personal information that travels across public networks and wirelessly
- Encryption of all personal information stored on laptops or other portable devices
- Education and training of employees on the proper use of the computer security system and the importance of personal information security

Detailed Written Information Security Policy—that includes:

Training, enforcing compliance with disciplinary measures, restrictions on physical access to personal information, a process to document breach response, annual assessment of program

Nevada

Requires the encryption of data sent outside of the secure system of the business (except facsimiles)

Practical Effect of the State Regulations

- Are they the new national standard?
- Can a CE or BA sign off on these verbatim?
- Does a HIPAA compliant program meet these requirements?
- Is encryption still addressable or mandatory (at least with respect to public networks, wireless and portable devices)?
- Breach notification will effectively be self-reporting of inability to comply
- Authorities have indicated a willingness to cooperate if companies are reporting breaches

New State Laws Post-HITECH

- New Hampshire has added a notification requirement for providers (and their BAs) that make an unauthorized disclosure of PHI; no risk of harm standard
- Virginia added a new law requiring state agencies to provide notice in the event of a breach involving medical information
- In sum, HITECH has not eliminated state action or involvement, but likely increased it with enforcement authority

Conclusion

- Be familiar with the laws governing protection of PHI/PI
- Prepare your breach response in advance
- Protect information to avoid a breach
- Communicate/Train/Discipline employees regarding privacy and security
- Increase oversight of BAs and those handling your employee data
- Address privacy and security thoroughly in your contracts