crowell moring

Who's Afraid Of A Big Bad Breach?

Security Breach Updates For Covered Entities And Their Business Associates

Christine Rinn
Barbara Ryland
Robin Campbell

September 16, 2009

Introduction

- American Recovery and Reinvestment Act of 2009
  - Makes significant changes to "administrative simplification" provisions of HIPAA regarding privacy and security
  - Increases the obligations and potential legal exposure of covered entities and business associates
    - New restrictions on the use and disclosure of protected health information (PHI)
    - HIPAA preemption will provide little (if any) relief in event of breach
  - Affords individuals more rights

Security Breach Provisions

Statutory definition of breach - The unauthorized acquisition, access, use or disclosure of protected health information, which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

Regulatory interpretation: "unauthorized acquisition… is "the acquisition, access, use or disclosure of protected health information in a manner not permitted under subpart E of this part."

Risk of Harm Standard & Limited Data Sets

- In the latest guidance 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".
- Thus, notification is necessary only if the breach poses a significant risk harm to the individual.
- Covered Entities (CEs) and Business Associates (BAs) must document their risk assessment to demonstrate that notification was not required.
- HHS also confirmed that PHI that excludes the 16 direct identifiers listed at 45 C.F.R. § 164.514(e)(2) and DOB and zip codes does not "compromise the security or privacy of PHI" due to the low level of risk associated with these limited data sets.

Examples

- PHI is impermissibly disclosed to another entity governed by HIPAA Privacy and Security Rules or to a Federal agency that is obligated to comply with the Privacy Act of 1974, there may be less risk of harm to the individual.
- A CE takes immediate steps to mitigate an impermissible use or disclosure, such as by obtaining satisfactory assurances from the recipient (for example, a confidentiality agreement or similar means) that the information will not be further used or disclosed or will be destroyed.
- A laptop is lost or stolen and then recovered and forensic analysis shows that it was not opened, altered, transferred or otherwise compromised.
- Type of information may also reduce risk, e.g. name and the fact that individual received services from a hospital (probably no harm), but if type of services is disclosed, or specialized facility, of if other more sensitive factor, like SSN, then notification will probably be required.

Exceptions

- HHS Guidance clarified the exceptions as follows:
- An unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a CE or BA, if such acquisition was in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.
- An inadvertent disclosure by a person who is authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CE or BA, or organized health care arrangement in which the CE participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.
- A disclosure of PHI where a CE or BA has a good faith belief that an unauthorized person to whom disclosure was made would not reasonably been able to retain such information.

Examples of Exceptions

- 1st Exception
- A billing employee receives and opens an email containing PHI about a patient which a nurse mistakenly sent to the billing employee. Billing employee alerts the nurse and deletes. Billing employee use of information was in good faith and within scope of authority, and would not constitute a breach provided there is no further disclosure.
- 2nd Exception
- A physician who has authority to use or disclose PHI at a hospital by virtue of participating in an organized health arrangement with the hospital is similarly situated to a nurse or billing employee at the hospital.
- 3rd Exception
- A CE sends EOBs to the wrong individuals, some are returned by the post office, unopened, as undeliverable—addressees could not have reasonably retained.
- A nurse hands a patient discharge papers for another, but quickly realizes and recovers the PHI from the patient. If patient did not read or otherwise retain, then no breach.

Information Covered

"Unsecured protected health information"

- PHI as defined by HIPAA (not limited to ePHI)
- Unsecured means:
  - Not secured through use of technology or methodology specified by the Secretary of HHS in guidance document; or
  - If no guidance is issued, then PHI not protected by a technology standard that renders PHI unusable, unreadable, or indecipherable that is developed or endorsed by a standards developing organization accredited by American National Standards Institute
- If "secured" acts as functional "safe harbor"—i.e. no need to notify under HITECH—but may have other state or federal obligations.

Initial Guidance by HHS on How to Secure Information

- 1) Encryption
- Encryption that meets one of the following standards (if the encryption key has not also been breached):
- --Valid encryption for data at rest consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies For End User Devices
- --Valid encryption for data in motion that complies with NIST Special Publications 800-52, Guidelines for Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs or others which are Federal Information Processing Standards (FIPS) 140-2 validated).

Initial Guidance by HHS on How to Secure Information (Cont.)

- 2) Destruction
- --Paper, film, or other hard copy media that has been shredded or destroyed such that PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of destruction.
- --Electronic media that has been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization, such that PHI cannot be retrieved.

Timeframe for Notification

- "Without unreasonable delay" and in no case later than 60 calendar days after discovery of breach (unless law enforcement requires delay) (could provide for timeframe shorter than 60 days)
- Clock starts ticking when 1st workforce member or agent knew, or by exercising reasonable diligence would have known
- CE must notify individuals within this time
- BA must notify CE within this time
- Note that if the BA is an "agent" of the CE, then the BA's knowledge is imputed to the CE and only one 60 day time period is applicable

Method of Notification to Individuals

- Written notice via US mail to individual or next of kin (or email if authorized)
- Substitute notice if there is insufficient or out-of-date contact information, if there are 10 or more individuals for whom there is insufficient contact information:
  - Conspicuous posting on website for a period of 90 days; or
  - Notice in major print or broadcast media (where individuals reside) (generally in the form of a press release)
  - If urgent, individuals may also be contacted by telephone
  - If utilizing substitute notice, must include a toll-free number that remains active for 90 days

Other Notifications

- If more than 500 residents *of a state or jurisdiction* are affected by breach, must notify prominent media outlets in that state or jurisdiction
- If more than 500 individuals in total are notified, Secretary must be notified immediately (i.e. within timeframe to individuals) (these will be posted on HHS website)
  - Instructions for notice to Secretary will be posted on website
- If less than 500 individuals, Secretary may be notified in an annual report
  - Instructions will be posted on HHS website
  - Must be provided no later than 60 days after the end of each calendar year
  - Log must be maintained for six years and made available to Secretary upon request

Contents of Notice

- Description of what happened, including date of breach and date of discovery, if known
- Description of type of PHI involved
- The steps individuals should take to protect themselves
- Description of what entity is doing to investigate, mitigate harm to individuals and protect against further breaches
- Contact procedures for more information, which must include a toll-free number, an email address, website, *or* postal address
- Must be written in clear, plain language

Requirements Beyond Notification

- CMS requirements for Medicare managed care organizations and Part D Sponsors
- Other requirements imposed by state regulators
- Contractual requirements (credit monitoring for agreed upon period, call center, credit restoration services, etc.)

CMS Requirements

- December 16, 2008 Memorandum
  - Security incident is the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.
  - Security incident includes potential loss of personally identifiable information (PII).
  - No risk of harm threshold.
  - CMS requirements apply to **both** beneficiary and provider information.
  - Notice to CMS may be required as quickly as within one hour discovery/detection.

Vendors and Service Providers

- Similar breach provisions are applicable to personal health record (PHR) vendors and their service providers, but oversight is provided by FTC rather than HHS.
- Definition of breach differs slightly--"with respect to unsecured PHR identifiable health information of an individual in a personal health record, acquisition of such information without the authorization of the individual".
- Must provide notice to individual and Federal Trade Commission, but FTC will notify HHS.
- In the event of a breach, a single entity may need to comply with the FTC breach notification provisions in its capacity as a PHR vendor, or make the required disclosure to a covered entity in its capacity as a business associate, or do both, depending on what PHI is compromised.

Effective Date

- Breach provisions effective 30 days after Secretary publishes interim final regulations, which are to be promulgated 180 days after date of enactment
- Effective date September 23, 2009
- Enforcement/Sanctions date February 22, 2010

Enforcement

- Penalties
- Enforcement action by Secretary
- Enforcement action by State AGs (but not during an ongoing federal action)

Preemption

- HIPAA preemption applies
- *Contrary* state laws are preempted, *unless they are more stringent* than the federal law
  - Contrary defined as "a CE could find it impossible to comply with both the State and federal requirements" or if the State law "stands as an obstacle to the accomplishment and execution of the full purposes and objectives" of the federal law
- Do state security breach laws fall within this preemption?
  - Most apply to entirely different set of information
  - Most have similar, not contrary provisions
  - Those which are contrary are generally more protective, e.g. 45 day timeline rather than 60 day

HHS Guidance provides that most state laws will not be preempted, e.g. shorter deadline for notice, differing content requirements.

Exemption

Few states offer total exemption for HIPAA regulated entities.

Most states provide an exemption for "a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this section shall be deemed in compliance with the notification requirements of this section if the person or business notifies affected persons in accordance with its policies in the event of a breach of the security of the system."

Other states provide an exemption for entities with breach policies dictated by federal law.

A few states remain with either no exemption or limited exemptions: AL, AR (CE's only), HI, MA, NY, NC, OH (CE's only), PR, VT, WY

Preemption/Exemption What's Left

- Evaluate the minimal obligations by statute, larger obligations through common law and state DTPA laws, and even larger obligations which stem from public and agency/authority relations
- Prepare a response plan/policy that will fall within the majority of state exemptions
- Include procedures in your policy that will satisfy the remaining states—plan content and CRA notification that will satisfy the majority
- Distinguish procedures for PHI breach with and without SSN
- Craft a single letter that meets the highest standard
- Alert state AGs when a breach includes a significant number of residents, CRAs when a significant number of SSNs are involved
- Don't forget that if you make a determination that there is no risk of harm under HIPAA breach rules, must still notify in CA, ND (DOB only), PR and TX which include PHI and have no risk of harm standard *unless exempt*

Interplay with State Laws

Information Covered

- Federal—Protected health information
- States—SSN, Driver's license and information that can lead to financial harm (CA, AR, MO, PR, TX apply to medical data, ND applies to DOB)

Harm Threshold

- Federal—added through guidance
- States—most do not require notification if there is no likelihood of harm

Content Requirements

- Federal—specific
- States—several require additional detailed information about fraud alerts, security freeze, contact information for agencies, etc.

Encrypted Data Exempt

- Federal—Yes
- States—There are still a few that do not exempt

Paper Breaches Exempt

- Federal—No
- States—Yes, all but seven do not include paper

Interplay With State Laws (Cont.)

Notice Requirements

- Federal—written is the same, threshold is lower for substitute notice, but means of substitute notice are easier
- States—written is the same, higher threshold for substitute notice, states require more than one method of substitute notice to be used

Timeline

- Federal—60 days or without unreasonable delay from covered entity to individual, 60 days or without unreasonable delay from business associate to covered entity (harsh discovery standard to start clock running)
- States—most have none, two have 45 days to individual, 10 days to owner if not owner

Notification to Authorities

- Federal—Secretary of HHS, FTC for vendors and service providers
- States—multiple authorities to notify—several states require notice to their AG, other state agencies, and law enforcement

Publication of Breach

- Federal—if greater than 500 residents of a state are affected, must notify major media, if greater than 500 people, must notify HHS who will post on website
- States—only a few states currently post breach notices on their websites, and notice to major media is only required when using substitute notice

Business Associates

- BAs are held to the same standards as CEs in the safeguarding, use and disclosure of PHI, including application of civil and criminal penalties, and including the new obligations that are enacted as part of the legislation.
- Certain types of entities are expressly defined as BAs, including Health Information Exchange Organizations, Regional Health Information Organization, E-prescribing Gateways, and Personal Health Record Vendors contracting with CE.
- Secretary is authorized to conduct audits of both CEs and BAs.

Minimum Necessary

- Creates temporary presumption that “minimum necessary” data is equivalent to the “limited data set.”
- An entity will be treated as being in compliance with the minimum necessary standard *only if*, to the extent practicable, it limits disclosure to a "limited data set" as defined under the Privacy Rule, or if necessary, to the "minimum necessary" data that is required to accomplish the intended purpose of the use or disclosure.
- Secretary is directed to issue regulations within 18 months of enactment, which will supersede the legislative standard.

Minimum Necessary

- The law appears to put an affirmative duty on covered entities to determine what information is minimally necessary if it contains additional elements.
- The interim final breach notification regulations specifically note that uses or disclosures that impermissibly involve more than the minimum necessary information may also qualify as breaches.

What To Do

- Address security breach in all future contracts and those up for renewal
- Consider amending existing contracts
- Prepare or revise your Incident Response Plan to include the new security breach provisions, which will possibly provide a state exemption
- Train, Train, Train not just on security and privacy, but specifics about security breach—examples of what constitutes a breach, how to report it, the importance of immediate action
- Be aware of nuances between CE/BA and Data Owner/Data Processor—CE/Data Owner has ultimate responsibility and control over notification to individuals

Incident Response Plan

Incident Response Plan

- Identify and train SIRT (Security Incident Response Team)
- Prepare templates (variations in letters)
- Investigate potential breach vendors in advance
- Identify critical contracts, notification deadlines
- Maintain contact lists: SIRT, Vendors, Clients
- Establish an escalation plan, often turns into a business, not legal, decision

Response Checklist

- Secure the information/systems
- Conduct investigation
- Involve law enforcement 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 to authorities (state AGs and others, HHS)
- Letters to CRAs
- Call Center FAQs/Call Script
- Vendor: Credit Monitoring, Notification

Contract Negotiation Basics

As a client hiring third party vendors to handle PHI:

- Address security breach directly in all relevant clauses
- Carve it out of any limitations of liability, limited warranties, exclusion of indirect or consequential damages, liability caps
- Set a contractual timeframe for notice of a breach shorter than statutory 60 days [48 hours after discovery, allows you to participate in investigation and response]
- Include a broad indemnification clause that covers any and all costs associated with a breach—not just those legally required (or at a minimum, leave these items up for negotiation post breach)
- Request notification for any incident involving your information (can be broader than PHI) and without any risk of harm evaluation by the BA), allows CE to "make the call" on risk
- Consider who should control the notification process

Contract Negotiation Basics (cont.)

As a vendor to a CE:

- Do not sign off as a BA unless you are truly acting as a BA under the law
- Limit security breach liability in all relevant clauses: limitations of liability, warranties, exclusion of indirect or consequential damages, liability caps

Q&A

Christine Rinn
crinn@crowell.com

Barbara Ryland
bryland@crowell.com

Robin Campbell
rcampbell@crowell.com

experience. creativity. results.