Keeping you "in the know" in the ASC industry

HOW TO EFFECTIVELY RESPOND TO A DATA BREACH

Kurt Bratten

O'CONNELL ARONOWITZ
ATTORNEYS AT LAW

THE HITECH ACT

- 2009 HEALTH INFORMATION AND TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH (HITECH) ACT
  - Expanded Privacy and Security Rules
  - Changed the breach standard (no more harm standard)
  - Increased penalties for violations
  - Business Associates (entities that create, receive, maintain, or transmit PHI on behalf of a CE) have increased obligations and independent liability

WHAT IS A BREACH?

- "an acquisition, access, use, or disclosure of protected health information in a manner not permitted under… [the Privacy Rule] is ***presumed*** to be a breach ***unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment…***"
  - A breach can only occur in connection with "unsecured protected health information" – essentially translates to unencrypted PHI
  - LIMITED EXCEPTIONS: (1) unintentional workforce access, (2) inadvertent disclosure to authorized person and (3) "good faith" belief that unauthorized person could not retain the data disclosed

HOW TO RESPOND TO A BREACH UNDER HIPAA

- Covered Entities and Business Associates can demonstrate a low probability that the PHI has been compromised based on a risk assessment that includes at least the following factors:
  1) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
  2) The unauthorized person who used the PHI or to whom the disclosure was made;
  3) Whether the PHI was actually acquired or viewed; and
  4) The extent to which the risk to the PHI has been mitigated.
- This incident-specific risk assessment must be documented
- May consider additional factors

HOW TO RESPOND TO A BREACH UNDER HIPAA

IN THE EVENT OF A BREACH, NOTICE MUST BE GIVEN TO:

1) All affected individuals
   - notice should be written but can be electronic, telephonic or by substitute notice
   - notification must be provided without unreasonable delay and in no case later than 60 days following discovery of a breach
   - written notice must include:
     - a brief description of the breach
     - a description of the types of data involved in the breach,
     - the steps affected persons should take to protect themselves from harm,
     - a brief description of what the CE is doing to investigate the breach, mitigate the harm, and prevent further breaches,
     - contact information for the CE (or BA, as applicable).

HOW TO RESPOND TO A BREACH UNDER HIPAA

IN THE EVENT OF A BREACH, NOTICE MUST BE GIVEN TO:

2) Prominent media outlets must be notified when more than 500 residents of a State or jurisdiction are affected

- media notice must be provided without unreasonable delay and no later than 60 days following discovery, and must include the information that affected individuals receive
- notice must be given to prominent media outlets within the State or jurisdiction more than 500 affected individuals reside

HOW TO RESPOND TO A BREACH UNDER HIPAA

IN THE EVENT OF A BREACH, NOTICE MUST BE GIVEN TO:

3) The Secretary of HHS, through OCR

- In addition to notifying affected individuals and the media, CEs must notify the Secretary by completing the online HHS form
- If a breach affects 500 or more individuals, CE must notify the Secretary without unreasonable delay and no later than 60 days
- If a breach affects less than 500 individuals, CE may notify the Secretary on an annual basis, reports of breaches affecting fewer than 500 individuals are due within 60 days of the end of the calendar year in which the breaches are discovered

HOW TO RESPOND TO A BREACH UNDER HIPAA

OTHER REQUIREMENTS IN THE EVENT OF A BREACH:

- A CE must mitigate any ongoing or harmful effects of a breach
- A CE must conduct a breach-incident assessment that identifies the causes and vulnerabilities involved in the breach and develops an appropriate remedial plan and remedial actions to address the causes and vulnerabilities associated with the breach incident and improves the CE's privacy and security protections
  - this breach assessment should include an analysis of these four factors in assessing the probability of data compromise: (1) nature and extent of the PHI involved; (2) the unauthorized person who used/accessed the PHI; (3) whether the PHI was actually acquired or viewed; (4) the extent the risk to the PHI was mitigated.

WHY COMPLY WITH HIPAA

- **Can be Criminal:** It is a federal crime to obtain or disclose PHI without authorization knowingly, under false pretenses or with intent to sell, transfer, or use PHI for commercial or personal gain or malicious harm.
- **Duty to Self-Report:** Business Associates must report breaches to Covered Entities and Covered Entities must self-report HIPAA breaches of unsecured PHI to the individual affected, HHS, and, when the breach affects 500 or more individuals, to the media.
- **Stiff Civil Penalties:** Federal Office for Civil Rights is required to impose HIPAA penalties if the Covered Entity or Business Associate acted with willful neglect (i.e., with "conscious, intentional failure or reckless indifference to the obligation to comply" with HIPAA).

CIVIL PENALTIES UNDER HIPAA

CONDUCT OF CE OR BA	PENALTIES
Did not know of violation and, by exercising reasonable diligence, would not have known	$100 to $50,000 per violation; Up to $1,500,000 per identical violation per year
Violation is due to reasonable cause and not willful neglect	$1,000 to $50,000 per violation; Up to $1,500,000 per identical violation per year
Violation is due to willful neglect but is corrected within 30 days after covered entity knew or should have known of violation	Mandatory fine of $10,000 to $50,000 per violation; Up to $1,500,000 per identical violation per year
Violation due to willful neglect and not corrected within 30 days after covered entity knew or should have known	Mandatory fine of at least $50,000 per violation; Up to $1,500,000 per identical violation per year

DATA SECURITY BREACH ACTION PLAN

1. Assign responsibility for breach response (Security Officer)
2. Train the assigned person and your workforce about breach reporting and applicable legal obligations
3. Create a breach response policy and procedure
4. Immediately collect all necessary data about the incident
   - names of involved workforce members and time of report
   - nature of the incident (systems, equipment and persons involved)
   - the way in which the incident was detected, including date/time the incident was first noticed
   - details about the origin of the attack or breach, IP address, name(s) and any information available about

DATA SECURITY BREACH ACTION PLAN

5. Designated breach response person or team must assess and begin documenting the incident:
   - Is the incident a reportable breach (real or perceived)
   - Is the incident still in progress and can it be quickly contained
   - The nature of the incident and whether outside assistance is needed (law enforcement, legal, information technology)
   - What data, assets and property is threatened and how critical is it, including impact an asset's loss would have on the business
   - The overall severity of the incident and its potential impact
   - The names and locations of the systems being targeted

DATA SECURITY BREACH ACTION PLAN

6. Investigate the incident immediately
   - Begin compiling a spreadsheet with contact information for all affected individuals and the types of PHI involved in the breach
   - Review all evidence, system activity and logs for relevant data
   - Interview witnesses, including all BA or workforce members
7. Develop a plan to mitigate any negative effects and securing all systems and PHI that were compromised
8. Implement plan and restore compromised systems and data, make necessary notifications and reports

DATA SECURITY BREACH ACTION PLAN

9. Document a risk assessment, including the following:
   - Summary of the incident, including key details, dates, discovery, etc.
   - If applicable, the origin of the breach or attack
   - Details of the response plan, mitigation efforts and investigation
   - Nature and extent that your PHI, data and records were involved
   - An assessment of the incident-specific risk
   - Conclusions and findings about whether the response was effective
   - Corrective and preventative actions taken
10. Take steps to make sure all evidence of the incident is preserved and not lost

RESOURCES

- HHS Web Page regarding Breach Notification:
  https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html
- HHS Frequently Asked Questions for Small Providers:
  https://www.hhs.gov/hipaa/for-professionals/faq/smaller-providers-and-businesses

QUESTIONS?

Kurt Bratten

(518) 462-5601
kbratten@oalaw.com

O'CONNELL ARONOWITZ
ATTORNEYS AT LAW

HIPAA Page Available on eSupport

- eSupport/Compliance/HIPAA

PROGRESSIVE SURGICAL SOLUTIONS

HOME ESUPPORT BLOG FORUM ACCOUNT

HIPAA: OVERVIEW

2016 WAS A RECORD YEAR FOR DATA BREACHES

It can happen to you

REFERENCE

Across all industries, the number of U.S. data breaches tracked in 2016 hit an all-time record high of 1,093, and in healthcare, troubling data security trends continue to plague the sector, according to new research from the Identity Theft Resource Center (ITRC) and CyberScout.

The number of breaches in 2016 represents a substantial hike of 40 percent over the near record high of 780 reported in 2015. Since 2005, the ITRC has been identifying data breaches in five industry sectors. In 2016, the business sector again topped the list in the number of data breach incidents, with 494 reported, representing 45.2 percent of the overall number of breaches. This was followed by the healthcare/medical industry (377 incidents), representing 34.5 percent of the overall total.

WHAT THIS MEANS:

The healthcare sector had the most records exposed by employee error or negligence. The healthcare industry was also the hardest hit by hacking, skimming and phishing attacks. So if you have not had a professional risk assessment done yet, get one done now! A formal risk assessment is required for all covered entities.

SEARCH

HIPAA

- **HIPAA Overview**
- Privacy vs. Security Officer
- Risk Assessment
- Disaster Recovery Plan
- Insurance Coverage
- Cell Phone Use

PROGRESSIVE SURGICAL SOLUTIONS

HOME ESUPPORT BLOG FORUM ACCOUNT

HIPAA: RISK ASSESSMENT

EHR INCENTIVES REQUIRE PROOF OF A FORMAL RISK ASSESSMENT

Risk Assessments are mandatory

REFERENCE

The Centers for Medicare and Medicaid Services (CMS) define a contingency plan as "an alternate way of doing business when established routines are disrupted." CMS offers the following seven steps as general guidelines for creating that plan: (1) assess your situation, (2) identify risks, (3) formulate an action plan, (4) decide if and when to activate your plan, (5) communicate the plan, (6) test your plan, and (7) treat your contingency plan as an evolving process.[1]

In addition to planning against disruptions in routines, healthcare entities are required to develop a HIPAA security contingency plan in the event of a security breach that jeopardizes PHI. HIPAA security standards require covered entities to "ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits" (§164.306(a)(1)) and to "protect against any reasonably anticipated threats or hazards to the security or integrity of such information" (§164.306(a)(2))

WHAT IT MEANS

This is not a new requirement. Risk Assessments have been a required for CEs since2006. If you thought your home grown "Excel" version of a risk assessment was enough – it's not. Risk Assessments take a full inventory of all your computers which are access points for data breaches, hackers and viruses. Most importantly a good risk assessment will take a scan from outside your CE and make sure that your network ports are secure and not open to hackers. This is very important. One open port is all a data hacker needs to start stealing PHI off your network.

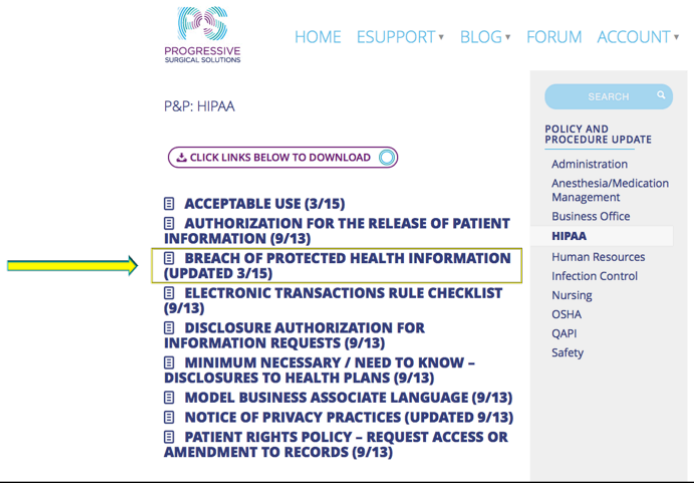
SEARCH

HIPAA

- HIPAA Overview
- Privacy vs. Security Officer
- **Risk Assessment**
- Disaster Recovery Plan
- Insurance Coverage
- Cell Phone Use

Available on eSupport

- eSupport/Compliance/Policy & Procedure Update/HIPAA



Still not an eSupport member?

Join the community…request your free web demo today!

- Visit www.progressivesurgicalsolutions.com/esupport
- Email us at **info@pss4asc.com**
- Or call us! **(855) 777-4272**

PROGRESSIVE SURGICAL eSupport

Mark Your Calendars

July 24, 2017 11am PT/ 2am ET

PURCHASING AND SUPPLY CHAIN

Brian Valley
McKesson

September 18, 2017 11am PT/ 2am ET

MINIMIZING THE RISK OF LEGAL CLAIMS/LIABILITY

Will Miller

Mark Your Calendars

August 25, 2017 11am PT/ 2am ET

COMPOUNDING PHARMACIES

Prima Pharma

$75
or
FREE
for eSupport members