

HIPAA Breach Lessons Learned

HCCA Mountain Conference 2018
Lyn Snow, MPA, CHC

Urgency

- My emergency is not necessarily other people's emergency



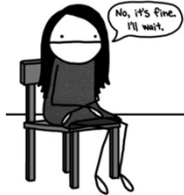
Authority

- What decisions can I make?
- What decisions require a higher level of approval?



Forensic Analysis

- Have the capability to perform a forensic analysis
- Know turnaround expectations



Be Proactive

- Have a toll free line in place
- Have a draft patient notification letter
- Draft a media notification



Policies, Procedures, Policies, Procedures

- Relevant
- Updated
- Policy in place at the time of the incident



Training

- Have a system in place to document training
- Provide content of the actual training
 - By employee
 - By date taken



Sanctions

- Verification of sanctions
- Signatures of employee & supervisor



Mail

- Be able to verify date of postmarked mail
- And personally delivered patient notification letters



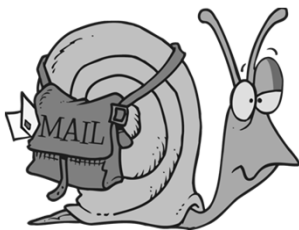
Say You Are Sorry



60 Days Goes By Fast



Waiting for your OCR resolution letter goes by slowly



Questions?

In the Trenches with HIPAA and
HI TECH
Valley View Hospital Association

Vicki L. Dwyer, RN, MN, CPC, CHC
Chief Compliance & Risk Officer
Valley View Hospital Association
1906 Blake Ave. Glenwood Springs, CO 81601
970-384-7043
Vicki.Dwyer@VVH.org

Valley View Hospital Association
In the Beginning – Fall 2013

- New CIO and Director of IT Fall 2010
- November 2013 – Complaints from Users
 - network was very slow and getting worse
 - Files being “Lost”
- Engaged a Forensics Team
 - Malware on several devices (started in registration)
 - Software creating “files” on system and encrypting them

**Valley View Hospital Association
First Corrective Actions – 2014**

- Shut ENTIRE System Down
 - Updated antivirus, antimalware software purchased and installed
 - Found all the files and decoded them
 - Implemented credit monitoring for all individuals affected
- Looked at other Technology to Host Patient Medical Record and Billing systems.

**Valley View Hospital Association
What Happened?**

- Someone (probably in registration) brought in a device and connected it to the server or clicked on an e-mail.
 - It appeared that the “files” never left Valley View and were not a direct “threat”.
- Antivirus software was outdated on some PCs
 - New software had been purchased but not deployed

**Valley View Hospital Association
What Happened?**

- The infected device copied all exe files and replaced them with their own files creation a # of files with PHI on different PCs
 - 172 computers infected with virus
 - On 90 computers, the virus recorded screen shots of selected secured web pages then hid the data in an encrypted file on the hard drive of the infected computers.
 - These files were programed to send information to a service in Amsterdam – the fire wall showed the “could have” gone out.
 - Breach involved 5415 individuals

Valley View Hospital Association Continued Corrective Actions

- 2014
 - Updated HIPAA Policies & Procedures
 - Provided HIPAA Education through On-line Learning system
 - Risk Assessment and Gap Analysis was done on systems to correct issues.
- 2016 & 2017
 - Revised/updated HIPAA Policies & Procedures
 - Updated HIPAA Education
 - Continued Risk Assessment and Gap Analysis on Annual Basis.
 - Hired HIPAA Security Office that reports to Compliance

Valley View Hospital Association Self-Disclosure of Potential Breach

- Self-Disclosure of Potential Breach
 - Breach was self-reported to the OCR on March 14, 2014.
- Response from OCR – August 18, 2014
 - 15 days to respond (from date of letter)
 - Data Request
 - A list of 22 items to be compiled and sent including:
 - Policies & Procedure,
 - HIPAA Training,
 - Implemented Security measures

Valley View Hospital Association

- 2nd Request for Information from OCR **March, 10, 2016**
 - List of 12 items to be submitted by **April 15, 2016**.
- 3rd Request for Information from OCR, **June 26, 2017**.
 - Policies & Procedures
 - Training
 - Statement of Operations and Balance Sheet
 - Availability of Insurance
 - Factors mitigating fine
- Investigation Closed by OCR in September 2017 with no fines.

Valley View Hospital Association Attorney-Client Collaboration

- Understanding what happened.
- Creating a Plan and Response to the OCR requests.
- Standardizing Policies and Procedures.
- Standardizing and Conducting HIPAA Training
- Developing a Response to the OCR
- Open Communications between Legal Counsel, Compliance & the OCR

Lessons Learned

- Open Communication between Compliance, IT, Legal
- Ensuring actions are still taking place, policies are updated, etc.
- Separating the HIPAA Privacy Officer from IT.
- HIPAA Compliance Audits & annual Training

SunHawkConsulting.com

SUNHAWK

BUSINESS ASSOCIATES IN THE CROSSHAIRS – THE UNPREDICTABLE BREACH

HCCA DENVER REGIONAL REGIONAL

OCTOBER 19, 2018



WHO ARE OUR BUSINESS ASSOCIATES?

SUNHAWK

Definition of Business Associate (BA) (45 CFR 160.103)

- A “business associate” is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information (PHI).
- A “business associate” also is a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate.

25

BUSINESS ASSOCIATE’S CONTRACT WITH COVERED ENTITY

SUNHAWK

164.504(e) – Business Associates Contracts (CEs protection)
HIPAA Standards for BAs/OCR Audits

The HIPAA Rules generally require that covered entities and business associates enter into contracts with their business associates to ensure that the business associate will appropriately safeguard protected health information.

2

6

HIPAA REQUIREMENTS FOR THE BA CONTRACT

SUNHAWK

Covered entities must **require** their business associate to:

- Maintain the privacy of protected health information
- Limit the use or disclosure of PHI to those purposes authorized by the covered entity (minimum necessary)
- Assist covered entities in responding to individuals requests concerning their PHI

The OCR has published sample BA language on its website.

27

[HHS.Gov/OCR/Privacy/HIPAA/Understanding/covered-entities/contractprov.html](https://www.hhs.gov/ocr/privacy/hipaa/understanding/covered-entities/contractprov.html)

WHAT HIPAA DOES NOT REQUIRE IN BA CONTRACTS

Covered entities are **not required** of their business associates by contract:

- Indemnity provisions
- Requirements to carry insurance

28

IF COVERED ENTITIES REQUIRE MORE...

Business associates may want to add terms to limit their liability, such as:

- Liability caps,
- Mutual indemnification, etc.

29

BREACH NOTIFICATION BY A BUSINESS ASSOCIATE

45 CFR 164.410

- A business associate shall, following the discovery of a breach or unsecured protected health information, notify the covered entity
- A breach shall be treated as discovered as of the first day on which such breach is known to the BA or, by exercising reasonable diligence, would have been known to the BA
- A BA is deemed to have knowledge of the breach if the breach is known, or be exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the BA

30

BREACH NOTIFICATION BY BA, CONTINUED

- Except as provided in CFR 164.412 (law enforcement delay), a BA shall provide the notification required without reasonable delay and in no case later than 60 calendar days after discovery of a breach (State law may differ)
- The notification shall include, to the extent possible, the identification of each individual whose unsecured PHI has been, or is reasonably believed by the BA to have been accessed, acquired, used, or disclosed during the breach
- A BA shall provide the covered entity with any other available information that the CE is required to include in notification to the individual under CFR 164.404(c) at the time of the notification or promptly as information becomes available

31

HIPAA 18 UNIQUE IDENTIFIERS

- 1) Name
- 2) Address (all geographic subdivisions smaller than state, including street address, city, county, and zip code)
- 3) All elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age if over 89)
- 4) Telephone numbers
- 5) Fax numbers
- 6) E-mail addresses
- 7) Social Security numbers
- 8) Medical Record numbers
- 9) Health plan beneficiary numbers

32

HIPAA UNIQUE IDENTIFIERS, CONTINUED

- 10) Account numbers
- 11) Certificate/license numbers
- 12) Vehicle identifiers and serial numbers including license plate numbers
- 13) Device identifiers and serial numbers
- 14) Web Universal Resource Locators (URL's)
- 15) Internet Protocol (IP) address numbers
- 16) Biometric identifiers including finger and voice prints
- 17) Full face photographic images and any comparable images; and
- 18) Any other unique identifying numbers, characteristic, or code

33

RISK OF HARM ANALYSIS

Risk of Harm analysis:

The Omnibus Rule modified the Breach Notification Rule to eliminate the former harm analysis. Now a breach of PHI is presumed to be reportable unless the CE or BA can demonstrate a low probability that the data has been compromised through an assessment of certain risk factors) 45 CFR Section 164.402;78 FR 5641 (1/25/13).

34

FOUR RISK FACTOR ANALYSIS

- The nature and extent of the PHI involved in the incident (sensitive information like social security numbers or infectious disease test results)
- The recipient of the PHI
- Whether the PHI was actually acquired or viewed
- The extent to which the risk that the PHI was compromised has been mitigated following unauthorized disclosure (whether it was immediately sequestered and destroyed)

35

IMPLEMENT REASONABLE AND APPROPRIATE POLICIES AND PROCEDURES

- 164.316(a): Requires written policies and procedures to comply with the HIPAA Rule and Standards
- 164.306(b): Policies and procedures based on the Business Associate's:
 - Size and capacity
 - Technical infrastructure
 - Cost of security measures
 - Potential risk to ePHI

36

SUGGESTED BA POLICIES – NOT EXHAUSTIVE






- HIPAA Use and Disclosure of Protected Health Information (PHI)
- HIPAA Password Management and Log-In Protection Policy
- HIPAA Clean Desk Policy
- HIPAA Breach Notification Policy – Business Associate
- HIPAA Access Control Policy
- HIPAA Confidentiality of Protected Health Information (PHI)
- Designation of HIPAA Privacy/Security Officer
- Accounting of Disclosures of Protected Health Information (PHI)
- HIPAA Workforce Training Policy
- Documentation and Record Retention Policy

37

HERE TO HELP - ANY QUESTIONS?



Jan Elezian, MS, RHIA, CHC, CHPS
Director & HIPAA Practice Leader
SunHawk Consulting, LLC   
Jan.Elezian@SunHawkConsulting.com

Jan has extensive experience in the Healthcare Health Information Management (HIM)/Compliance/HIPAA/Meaningful Use and Revenue Cycle areas. During her 40 years in the Healthcare industry Jan has provided Healthcare Regulatory, Compliance and Investigative services, serving in various administrative roles. Most recently, Jan served as Associate Vice-President and Corporate Compliance Officer at an integrated healthcare system in Scottsdale, Arizona. Jan has experience in various HIPAA Privacy and Security and Meaningful Use assessments which included workflow reviews, data flow reviews, strategy formation, and governance decision and guidelines. Jan has performed or overseen over 200 privacy investigations and was involved in the development of an integrated HIPAA Security breach response plan.

45
