

Only You Can Prevent HIPAA Breaches!

Jill Jensen, J.D.

Nebraska Hospital Association
Annual Convention
October 26, 2017



Jill Jensen, J.D.

CLINE WILLIAMS
WRIGHT JOHNSON & OLDFATHER

Attorney

jjensen@clinewilliams.com

Direct: 402-479-7116

Fax: 402-474-5393



Recent Enforcement Actions

HIPAA Audits Update

Recent Entries/Candidates for the
“Wall of Shame”

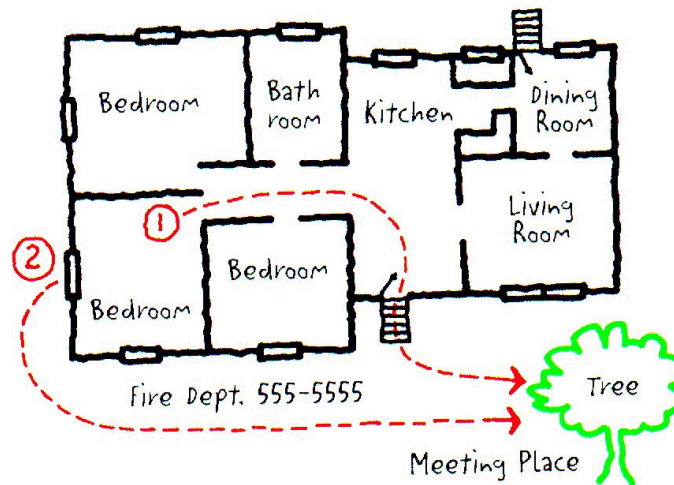
Limiting Your Risk of a Breach



If you do find
matches, give
them to an
adult.



**Have an
escape
plan with
a family
meeting
place.**



**If your clothes catch on
fire . . .**



Stop



Drop



Roll

So, what does this have to do with HIPAA and preventing HIPAA breaches?



The lessons you learned as a kid still apply and

-- can help you limit your risk of a HIPAA breach.



Moral: Be safety conscious!

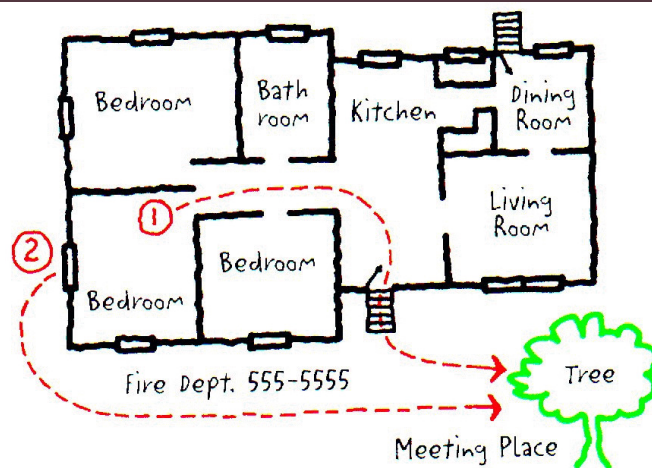
If you do find
matches, give
them to an
adult.

Do a HIPAA
risk
analysis-risk
assessment
regularly!



Moral: Have a plan!

Have an
escape
plan with a
family
meeting
place.



- ☐ How's your HIPAA compliance program?
- ☐ When was the last time you reviewed your HIPAA policies and procedures?

If your clothes catch on fire . . .

Moral: Take action!



Stop

When you detect a problem,
deal with it!



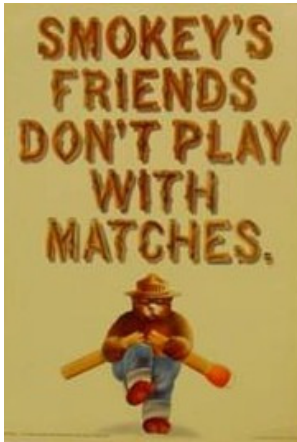
Drop



Roll

Recent Enforcement Actions





Being Safety Conscious – Using Your Head

Using Your Head



- St. Luke's-Roosevelt Hospital Center Inc.
- Complaint received by OCR in Sept. 2014
- OCR investigation
- Two patients affected
- Involved failing to safeguard PHI when faxing information
- \$387,200 Resolution Amount and CAP

Being safety conscious when faxing PHI

- Patient # 1
- Staff member disclosed HIV status of individual to the individual's employer
- Impermissibly faxed PHI to employer rather than sending it to the requested personal post office box.



Patient #1's PHI

- Included
 - Medical care
 - STDs
 - Medications
 - Sexual orientation
 - Mental health diagnosis, and
 - Hx of physical abuse

Patient # 2

- Another individual's PHI faxed to an office where the individual volunteered
- OCR characterized both breaches as "egregious" because of the type of information involved
 - HIV, AIDS, and mental health



The Result?

- \$387,200 Resolution Amount
- Corrective Action Plan
 - 3 years
 - Review and revise as necessary HIPAA policies and procedures
 - Distribute same to workforce
 - Workforce certification of having read/understood
 - Training + workforce certification of being trained



Being Safety
Conscious –
Another
example

Watch what you put in a
press release

- Memorial Hermann Health System,
Houston, TX
 - Largest nonprofit health system in
southeast Texas
 - 16 hospitals
 - 24,000 employees
- October 2015 OCR compliance review
based on multiple media reports of
unauthorized disclosure



~~What w~~ Were they thinking?

- Patient's PHI released to 15 media outlets/reporters in Sept. 2015
- Senior leaders disclosed Patient's PHI in 3 meetings with advocacy groups, state legislators
- Also disclosed PHI on website
- All without the patient's authorization
- Did not document timely sanctions against those responsible



The Backstory

- The patient was 44-year old woman, an illegal alien from Mexico who was arrested at a gynecologist's office after presenting a fake ID
- She had lived in the Houston area for 12 years
- Had no record of prior arrests. Clinic staff called police.
- Protestors of the incident stood outside of the medical office and said hospitals, as well as churches, should be safe zones
- MHHS subsequently published a press release with the patient's name in the title



- \$2.4 Million Resolution Amount
- Corrective Action Plan for 2 years
- Develop, maintain, and revise as necessary HIPAA policies and procedures
 - Implement
 - Distribute to workforce and obtain certification
- Specific requirement of policies/procedures for uses/disclosures of PHI where authorization required including to media, public officials
 - Also, law enforcement disclosures and health oversight activities

Corrective Action Plan Requirements

- Identify persons that workforce members may contact in the event of inquiries or concerns about HIPAA compliance
- Internal reporting procedures requiring all workforce members to report to designated person or office at “earliest possible time” any potential violations of HIPAA Privacy or Security or Breach Notification Rules
- Must require prompt investigation
- Applicable and documentation of sanctions
 - Retraining
 - Other corrective action
 - For workforce
 - Including senior management
 - Very prescriptive

OCR's prescription for success for MHHS:

- “This content shall include”
- Description of the sanctions
- Timeframe in which MHHS will apply and document sanctions for violations of the HIPAA Rules or of MHHS' privacy, security or breach policies or procedures
- Manner in which MHHS will document the sanctions; and
- Where MHHS will store or retain the documentation (e.g., personnel file).



Being Safety Conscious –
Doing a Risk
Assessment/Risk Analysis

Risk Assessment/Risk Analysis

What is it?

§164.308 Administrative safeguards.

(a) A covered entity or business associate must, in accordance with §164.306:

(1)(i) *Standard: Security management process.* Implement policies and procedures to prevent, detect, contain, and correct security violations.

(ii) *Implementation specifications:*

(A) *Risk analysis (Required).* Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

OCR says that conducting a risk analysis is

- “the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule. Therefore, a risk analysis is foundational,”
- “An organization should determine the most appropriate way to achieve compliance, taking into account the characteristics of the organization and its environment.”
- No “one size fits all” blue print
- “methods [of risk analysis] will vary dependent on the size, complexity, and capabilities of the organization.”



- April 2017 Resolution Agreement with OCR
- FQHC in Denver – serves 43,000 patients, many low income
- Access to ePHI of 3200 patients

With no risk analysis

- MCPN had not implemented risk management plans to address risks and vulnerabilities
- When MCPN finally conducted a risk analysis, that risk analysis, as well as all subsequent risk analyses, were insufficient to comply with Security Rule.
- Too little
- Too late

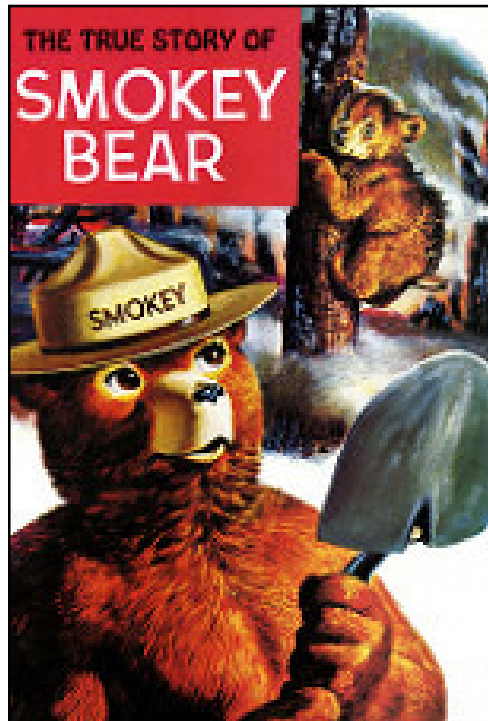
No Risk Analysis

- HIPAA violation because FQHC failed
 - to conduct an accurate and thorough risk analysis, and
 - to implement a risk management plan sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level
- “relatively low” resolution amount of \$400,000 – OCR considered FQ status

What happened?

- Breach report filed in Jan. 2012
- Hacker accessed ePHI through employee email
- Phishing incident
- Failed to do a risk analysis until Feb. 2012





Being Safety Conscious – Doing a Risk Analysis/ Risk Assessment



- April 24, 2017
- First settlement involving a wireless health services provider
- Laptop stolen from workforce member's parked car
- HIPAA security policies and procedures in draft form – no final policies



- 2 Breaches of ePHI - in Jan. and Feb. 2012 with 1391 and 2219 patients affected
- Failed to conduct an “accurate and thorough” risk analysis
- Failed to plan for and implement security measures to reduce risks



- Failed to
 - implement policies and procedures about receipt/removal of hardware and electronic media in and out of its facilities, encryption of media, and movement internally until March 2015
 - have safeguards to prevent unauthorized disclosures/access to employees
 - take steps to correct unauthorized internal disclosures

Conduct a
risk analysis



Develop & implement a
risk management plan

- \$2.5 Million Resolution Amount
- Corrective action plan for 2 years
- Implement secure device and media controls
- Review/revise employee training program

Tool for
risk analysis

<https://www.healthit.gov/providers-professionals/security-risk-assessment-tool>



Downloadable Tool

- For Windows
- For iPad
- 156 questions
- Also a paper version
- User Guide

Professionals > Privacy & Security > Security Risk Assessment > Security Risk Assessment

Risk Assessment

Security Risk Assessment Tool


What is the Security Risk Assessment Tool (SRA Tool)?

The Office of the National Coordinator for Health Information Technology (ONC) recognizes that conducting a risk assessment can be a challenging task. That's why ONC, in collaboration with the HHS Office for Civil Rights (OCR) and the HHS Office of the General Counsel (OGC), developed



<https://www.healthit.gov/providers-professionals/security-risk-assessment-tool>

- Resources with each question to help:
 - Understand the question's context
 - Consider the potential impacts if the requirement not met
 - See the actual safeguard language of the HIPAA Security Rule
- Can document answers, comments, and risk remediation plans in the tool – information not sent somewhere else
- It's free



Security Risk Assessment Tool

[Tutorial](#)

Current User: JGJ | [Logout](#) | [www.HealthIT.gov](#)

A01

§164.308(a)(1)(i) - Standard
Does your practice develop, document, and implement policies and procedures for assessing and managing risk to its ePHI?

☒ Yes
 ☐ No
 ☐ Flag

Current Activities	Notes	Remediation

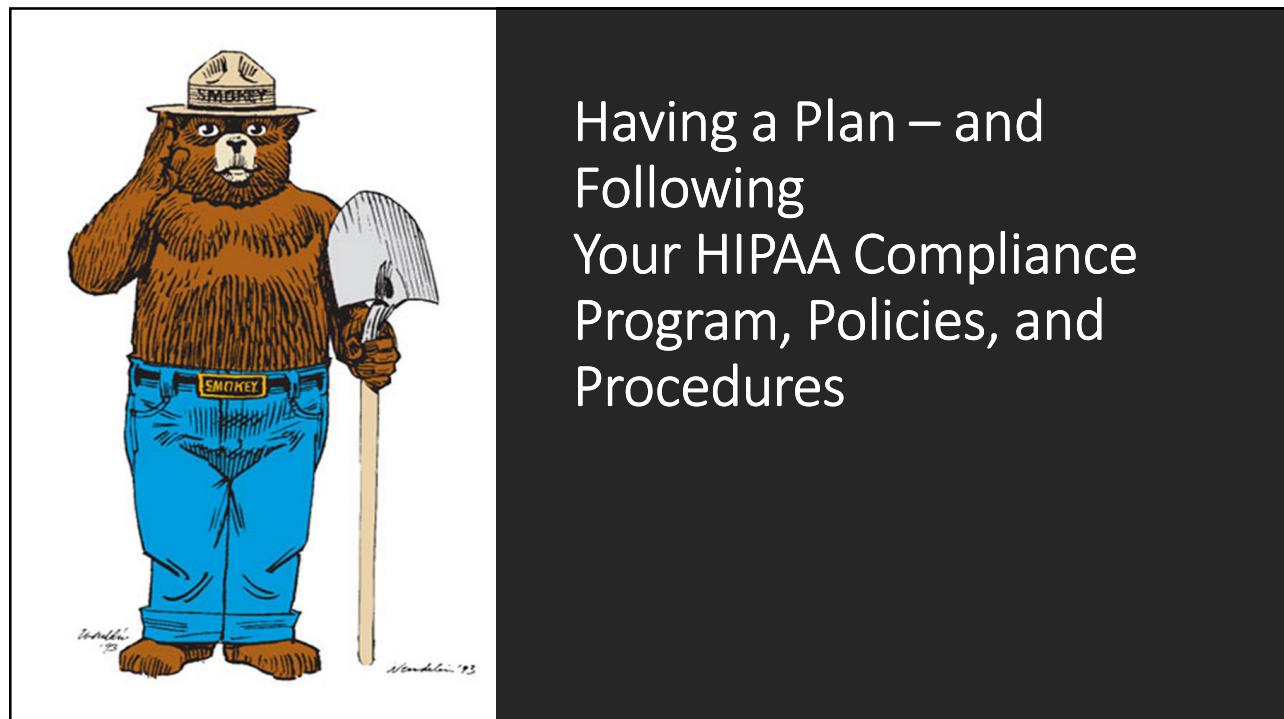
With respect to a threat/vulnerability affecting your ePHI:

Likelihood: ☐ Low ☒ Medium ☐ High

Things to Consider

An information system is an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and users.

A portable electronic device is any electronic apparatus with singular or multiple capabilities of recording, storing, and/or transmitting data, voice, video, or photo images. This includes but is not limited to laptops, personal



What happens when you don't have a plan



- ☐ \$2.5 Million
- ☐ Corrective Action Plan for 2 years
- ☐ 2 breach reports – April and July 2012
- ☐ 115,143 patients affected
- ☐ Feb. 2017 settlement

Modern Healthcare

The leader in healthcare business news, research & data



One way to make *Modern Healthcare*



The Facts

- 2 employees impermissible access to PHI
- Names, DOB, SSN
- Internal investigation found additional 12 other employees
- Affecting 115,143 patients

What Went Wrong

- Former employee of physician practice had access to PHI of 80,000 patients for over a year
- Failed to implement procedures to regularly review records of information system activity
 - audit logs
 - access reports
 - security incident tracking reports
- Jan. 1, 2011 through June 2012

From the HHS Press Release

- . . . MHS failed to regularly review records of information system activity on applications that maintain electronic protected health information by workforce users and users at affiliated physician practices, despite having identified this risk on several risk analyses conducted by MHS from 2007 to 2012.
- The login credentials of a former employee of an affiliated physician's office had been used to access the ePHI maintained by MHS on a daily basis without detection from April 2011 to April 2012, affecting 80,000 individuals.

What went wrong?

- January 1, 2011 until June 1, 2012
- Did not “implement” policies and procedures (i.e., “failed to follow”)
- Had access authorization policies
- Did not establish, document, review, and modify a user's right of access as required by 45 C.F.R. § 164.308(a)(4)(ii)(C).
- \$5.5 Million Resolution Amount
- Corrective Action Plan – 3 years



Corrective Action Plan elements

- Complete a risk analysis and risk management plan
- Revise policies and procedures
 - Information system activity review to require the regular review of audit logs, access reports, and security incident tracking reports
 - Access establishment, modification, termination
 - Protocols for access to MHS's e-PHI by affiliated physicians, their practices, and their employees
- Regarding risk analysis and risk management, review and revise existing policies and procedures for compliance
- Submit to HHS

The Importance of Taking Action



What happens when you don't take action

- Children's Medical Center, Dallas, TX
- 3 hospitals and many clinics in north Texas
- Filed a breach notification report in Jan. 2010 about the loss of an unencrypted Blackberry in Nov. 2009
- Had ePHI of 3800 persons
- OCR began its investigation in June 2010

Children's Medical Center, Dallas

- During OCR investigation, Children's submitted GAP analysis done by a vendor Strategic Management System ("SMS") in Dec. 2006-Feb. 2007 for Children's
- Identified lack of risk management as a major finding
- Recommended encryption for laptops in case of loss or theft
- Separate analysis of risks and vulnerabilities to ePHI by Pricewaterhouse Coopers ("PwC") in Aug. 2008
 - Identified high risk because of potential loss of unsecured devices
 - Recommended encryption

What went wrong?



- Despite the recommendations, allowed workforce to use unencrypted devices through April 2013
- Knew there was a problem and did not fix it.
- By Nov. 2012,
 - did not put in place an alternative or document why it did so
 - did not implement policies/procedures to govern movement of data, media, and hardware containing ePHI into, out of, and within the facility
- No inventory of devices to which media control policy would apply

What else?

- iPod of workforce member lost in Dec. 2010 – OCR notified
- Synced to email at work
- ePHI of 22 persons
- Not encrypted



There's more



- ☐ OCR findings in Sept. 2012 – Insufficient controls on USB drives and smartphones to prevent unauthorized USB to be taken out the hospital unencrypted resulting in a breach
- ☐ July 2013 breach notification report to OCR about a lost laptop – again, unencrypted
 - ☐ Had been password protected
 - ☐ Some security measures there with badge access and cameras

And more . . .



- But janitorial personnel not authorized to access ePHI had unrestricted access to the area where laptop was stored.
- Occurred between April 4 and 9, 2013
- 2462 persons' information
- Attempted informal resolution by OCR and Children's
- \$3,217,000 Civil Money Penalty
- Aggravating factors – Children's knew about the problems and did not fix them – the amount of time and prior hx of noncompliance



Moral to the story

- If you know you have an issue, you **must** take steps to get the problem fixed.
- If required, do it!
- If addressable, **determine** what you will do and **document** the **reasons** why the solution is appropriate



HIPAA Phase II Audits

Phase II HIPAA Audits: What's the point?

- Identify best practices; identify risks & vulnerabilities; Identify areas for guidance; encourage compliance
- Intended to be non-punitive, but OCR can undertake compliance review
 - If significant concerns are raised during an audit
 - Entity fails to respond
- Information from this phase to be used in developing ongoing audit program
- Also, to develop tools and guidance for industry self-evaluation and breach prevention



What's the status of the Phase II Audits?



- 166 Covered Entities
- 43 Business Associates
- Phase II audits of
 - Covered Entities -- Complete
 - Business Associates – Wrapping-up
- No onsite audits in Phase II
- Phase III will include onsite audits

What's Happening in the Phase II Audits?

- Summary report expected— maybe this year
- None of the Phase II auditees were moved to the compliance track
- There was a small number notified about audit but did not respond -- on a compliance track

U.S. Department of Health and Human Services
Office for Civil Rights
Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information

Please Note: The Breach Notification Portal will be offline for maintenance from Fri Jul 28 10:00 PM EDT to Sat Jul 29 07:00 AM EDT. Any information being entered when the Portal is taken off-line will be lost.

Under Investigation Archive Help for Consumers

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. The following breaches have been reported to the Secretary:

Cases Currently Under Investigation

This page lists all breaches reported within the last 24 months that are currently under investigation by the Office for Civil Rights.
[Show Advanced Options](#)

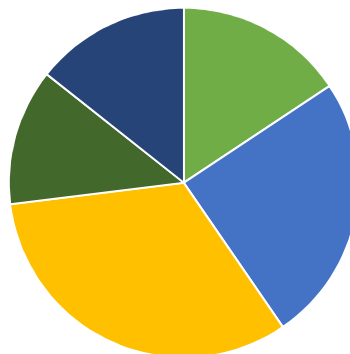
Breach Report Results							
Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
	Healthcare Provider		Healthcare Provider	571	07/21/2017	Hacking/IT Incident	Email
	Healthcare Provider		Healthcare Provider	1529	07/13/2017	Theft	Desktop Computer, Paper/Films
	Healthcare Provider		Healthcare Provider	2500	07/13/2017	Hacking/IT Incident	Electronic Medical Record
	Associates		Healthcare Provider	4391	07/11/2017	Unauthorized Access/Disclosure	Email
	LC&Z General and Cosmetic Dentistry	FL	Healthcare Provider	4391	07/11/2017	Unauthorized Access/Disclosure	Email
	White Coats Wellness	FL	Business	10000	07/10/2017	Hacking/IT Incident	Email

The Wall of Shame

Breach Barometer – 1st Half of 2017

233 Reported Breaches

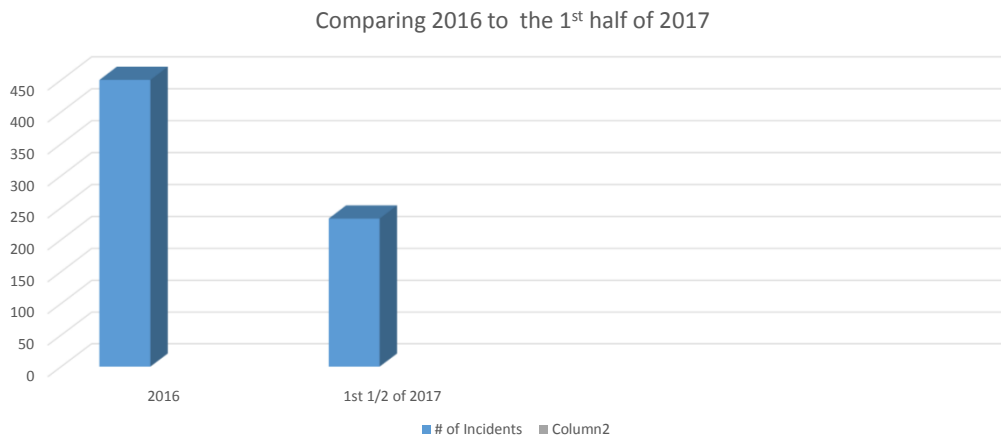
Breaches - Jan. - June 2017



Source: Protenus/Databreaches.net

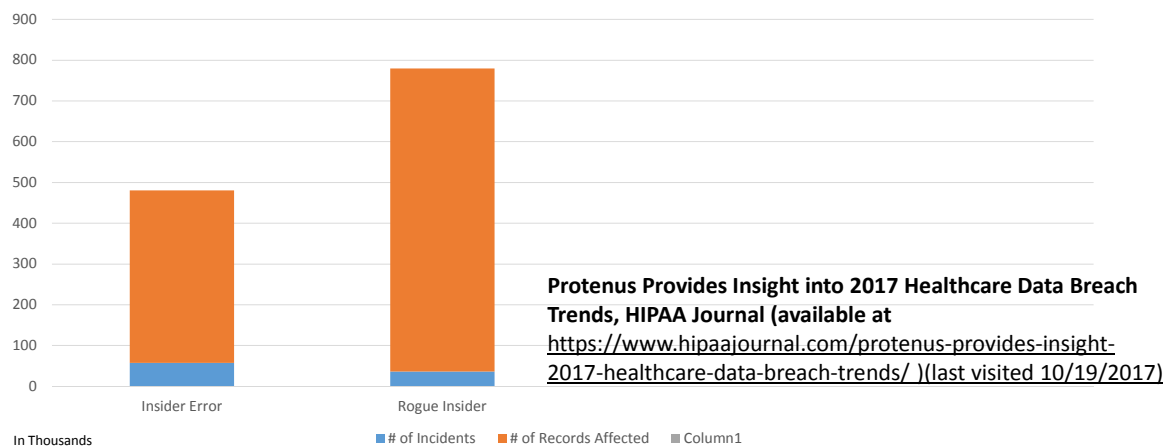
Protenus Provides Insight into 2017 Healthcare Data Breach Trends, HIPAA Journal (available at <https://www.hipaajournal.com/protenus-provides-insight-2017-healthcare-data-breach-trends/>) (last visited 10/19/2017)

More from the Breach Barometer By # of Incidents in 2016 compared to 1st Half of 2017



Protenus Provides Insight into 2017 Healthcare Data Breach Trends, HIPAA Journal (available at <https://www.hipaajournal.com/protenus-provides-insight-2017-healthcare-data-breach-trends/>) (last visited 10/19/2017)

Number of Patients Affected by Insider Breaches



Protenus Provides Insight into 2017 Healthcare Data Breach Trends, HIPAA Journal (available at <https://www.hipaajournal.com/protenus-provides-insight-2017-healthcare-data-breach-trends/>) (last visited 10/19/2017)

The Wall of Shame

- https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
- Common Themes:
 - Insiders – bad actors
 - Insiders - schlepitude
 - Ransomware
 - Phishing
 - Mobile device security – no encryption
 - Risk Analysis MIA
 - Risk Management MIA
 - Fixing what's broken before it becomes a problem



Limiting Your Risk of Breach

Workforce Training

- What uses/disclosures require an authorization?
- Do your people know?

Business Associate Agreements

- Current with HITECH?
- Signed for all Business Associates?

Risk Analysis/Risk Assessments

- Not done
- Done poorly
- No follow-up

Limiting Your Risk of Breach

Failing to manage the risks identified

- Taking timely action to fix issues identified
- Follow-up and follow-through

Device/Mobile device security

- Inventory
- Encryption

Transmitting PHI securely

- Email
- Texts
- Files
- Remote access



Think before you strike.



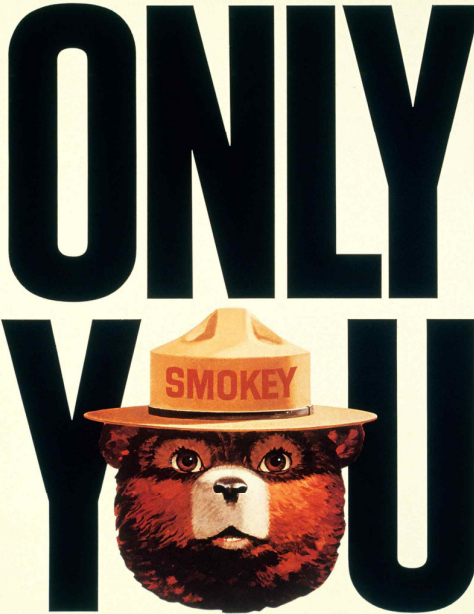
Limiting Your Risk of Breach

Auditing and monitoring access to PHI

Celebrities
Other employees
Family members of employees
Neighbors
Timing of access
Volume of access

Information Security Hygiene

Patching software
Use of unsupported software
Inventory and tracking
Encryption at rest and in transmission



Limiting Your Risk of Breach

- Insider threats**
 - Appropriate access for position
 - Training
 - Monitoring for bad actors
 - Access on-boarding/off-boarding
- PHI Disposal**
 - Copiers
 - Fax machines
 - Paper
 - Electronic

More risks

Disaster recovery

Back-ups that work and tested

Contingency planning



Let's be
careful out
there!



Your Questions

Thank you!

Jill Jensen, J.D.

jjensen@clinewilliams.com

Direct: 402-479-7116

Fax: 402-474-5393

CLINE WILLIAMS
WRIGHT JOHNSON & OLDFATHER