

# **HIPAA: Are We Doing This Right?!**

**Katie Ilten**

**Briar Andresen**

**Marguerite Ahmann**

**November 8, 2017**

**Fredrikson**  
& BYRON, P.A.

# Today's topics

- Current government enforcement
- HIPAA audits
- Obligations for security risk assessments
- Compliance updates, recent “clarifications” and waivers from the Office for Civil Rights.
  - Opioid guidance (and Part 2)
  - Hurricane
  - Charging for records/access
- Privacy Officers woes
  - Training
  - Breaches
  - BAAs

# Types of OCR Enforcement

1. Resolved after intake (no investigation)
2. Technical assistance (no investigation)
3. No violation (investigated)
4. Corrective action taken (investigated), possible settlement agreement and resolution amount (\$\$)
5. Civil money penalty
6. Referred to DOJ or other agency

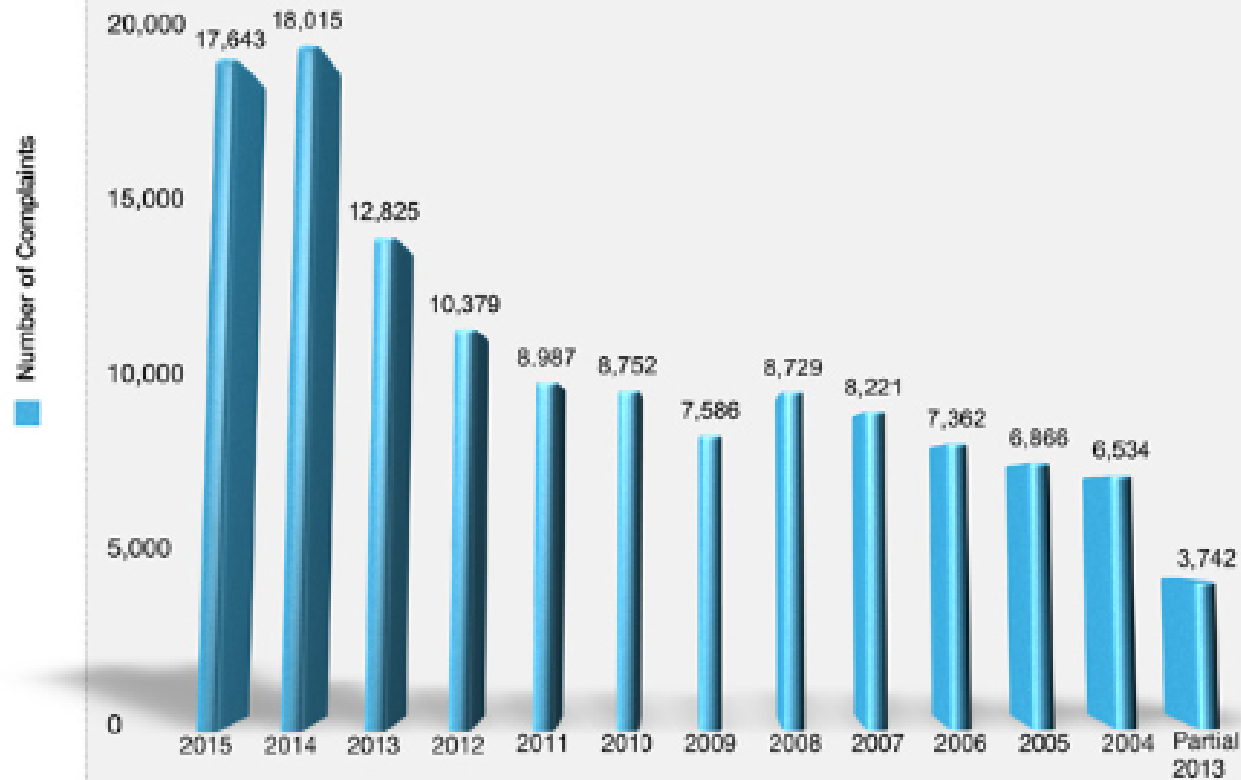
# The Numbers: Complaints

- No violation occurred: ~12,000.
- Over 25,000 investigations were resolved by corrective action.
- 52 corrective action cases have had a monetary settlement, with the total of all settlement amounts over \$72,000,000.
- Just a few civil money penalty cases.

# The Numbers: Complaints

- Since 2003, OCR has received over 165,000 complaints, resolving 97% in some manner.
- Complaint not eligible for enforcement: ~100,000.
- Approx. 23,000 were early intervention with technical assistance and no investigation.

## Complaints Received by Calendar Year

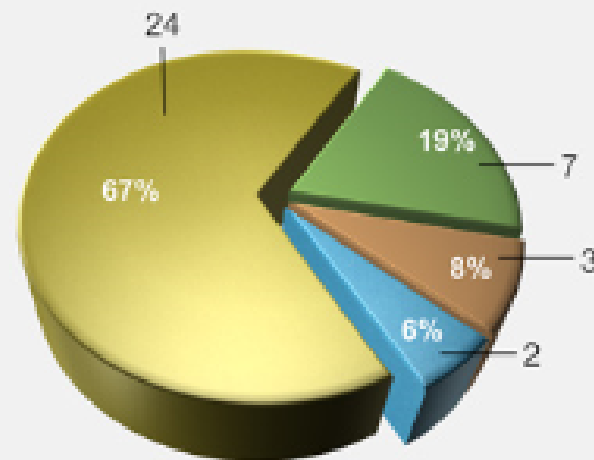


# The Numbers: Compliance Reviews

- OCR has initiated 841 compliance reviews since 2003.
- Most compliance reviews are initiated following a breach.

## CR Non-Breach Cases Closed

Year: 2015



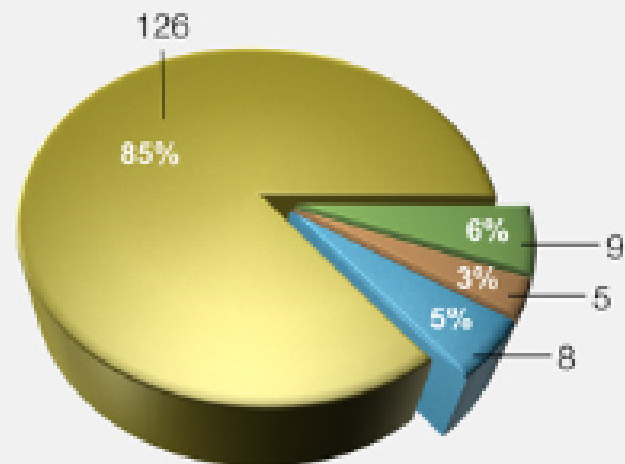
Total Resolutions: 36

- Other
- Investigated: Corrective Action Obtained
- Resolved After Intake and Review
- Investigated: No Violation



## CR Breach Cases Closed

Year: 2015



Total Resolutions: 148

- Other
- Investigated: Corrective Action Obtained
- Resolved After Intake and Review
- Investigated: No Violation

# Common Offenders

- Most common entities required to undertake corrective action (in order):
  - Private Practices
  - General Hospitals
  - Outpatient Facilities
  - Pharmacies
  - Health Plans

# HHS Wall of Shame

- Breakdown of breach by location
  - Paper records (22%)
  - Laptop (21%)
  - Desktop (12%)
  - Network server (12%)
  - Portable electronic device (11%)
  - Email (7%)
  - EMR (4%)
  - Other (11%)

# HHS Wall of Shame

- Breakdown by type of breach
  - Theft (51%)
  - Unauthorized access/disclosure (19%)
  - Loss (9%)
  - Hacking/IT incident (7%)
  - Improper disposal (4%)
  - Other (9%)
  - Unknown (1%)

# HIPAA audits

- “Phase Two” audits have been happening since July 2016
  - Review policies and procedures of CEs and BAs
  - Information gathering via email
  - OCR tried to look at broad spectrum of types of entities, but 90% were health care providers
  - Majority got privacy/breach audit, roughly 1/3 got security audit

# HIPAA audits

- CEs were asked to identify their BAs
  - OCR “encouraged” CEs to prepare a list of each BAA with contact info in order to respond...
  - Supposed to be wrapped up by end of 2016, followed by onsite audits in 2017
  - Some desk auditees would have onsite audit
  - Possible that significant findings would lead to separate compliance review from OCR
    - The bad kind

# HIPAA audits

- Onsite audits were supposed to start in 1<sup>st</sup> quarter of 2017
- They may not happen until 2018
  - Still assessing the results of the desk audits
- OCR's "preliminary" Phase 2 results of 166 CEs found that compliance was "inadequate," and over **94% of CEs failed to demonstrate appropriate risk management plans.**

# Ratings system

Compliance Effort Ratings—Legend	
Rating	Description
1	The audit results indicate the entity is in compliance with both goals and objectives of the selected standards and implementation specifications.
2	The audit results indicate that the entity substantially meets criteria; it maintains appropriate policies and procedures, and documentation and other evidence of implementation meet requirements.
3	Audit results indicate entity efforts minimally address audited requirements; analysis indicates that entity has made attempts to comply, but implementation is inadequate, or some efforts indicate misunderstanding of requirements.
4	Audit results indicate the entity made negligible efforts to comply with the audited requirements - e.g. policies and procedures submitted for review are copied directly from an association template; evidence of training is poorly documented and generic.
5	The entity did not provide OCR with evidence of serious attempt to comply with the Rules and enable individual rights with regard to PHI.



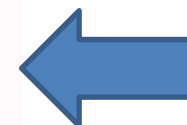
# Failure rates ☹️

Rated Inadequate or Worse	Topic
89%	Patient right of access or copy of their PHI
65%	Content of Notice of Privacy Practices
67%	Content of notice to individual that there has been a breach
83%	Perform an information security risk analysis
94%	Establish or maintain an information security risk management plan

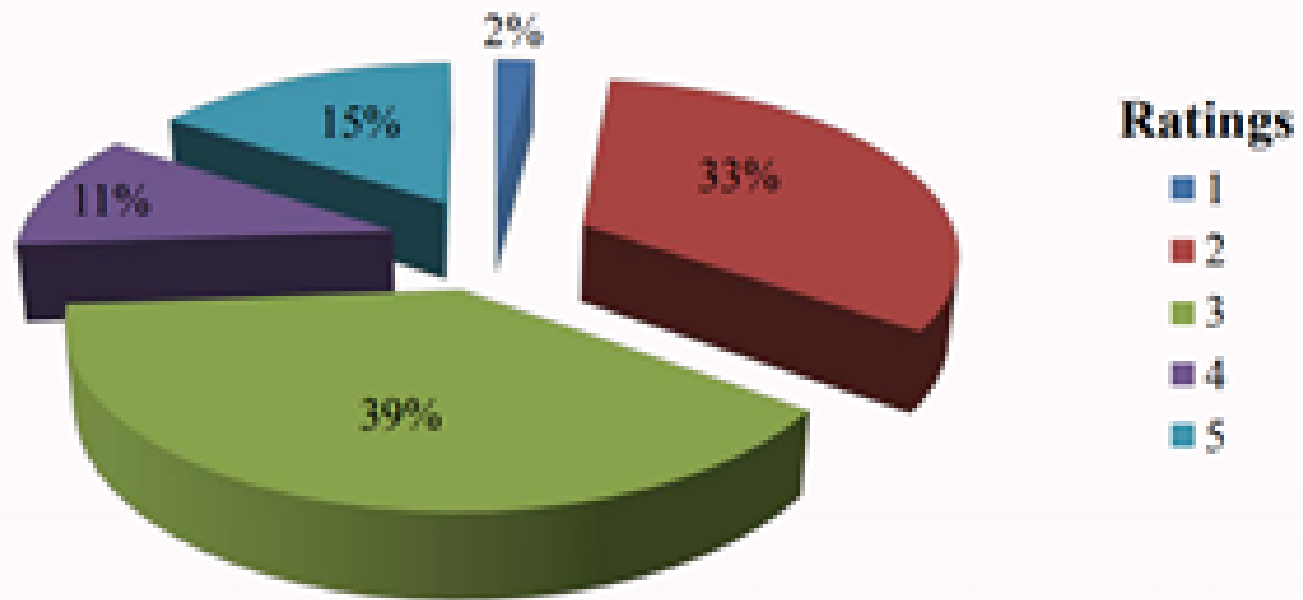
Table from Cynergistik.com

# Work to do

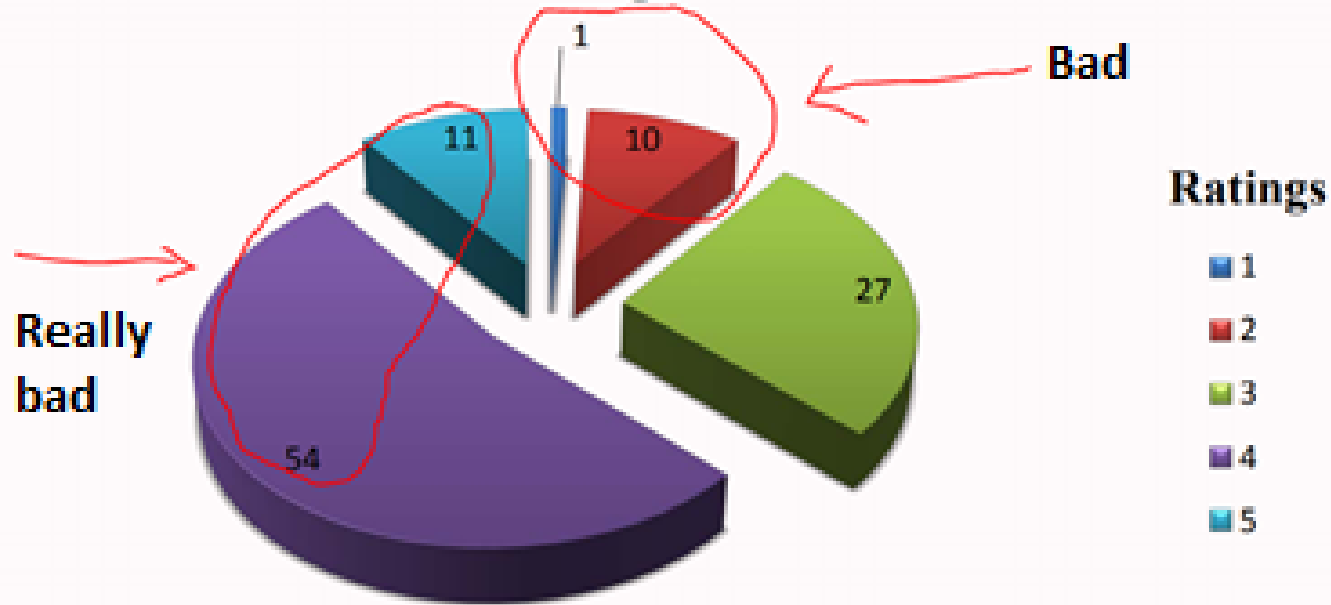
Rating Poles		
Breach T 103	5 Rating	1 Rating
Timeliness of Notification	15	67
Content of Notification	9	14
Privacy T 103		
Access	11	1
Notice Content	16	2
eNotice	15	59
Security T 63		
Risk Analysis	13	0
Risk Management	17	1



## P55 – Notice of Privacy Practices – Content

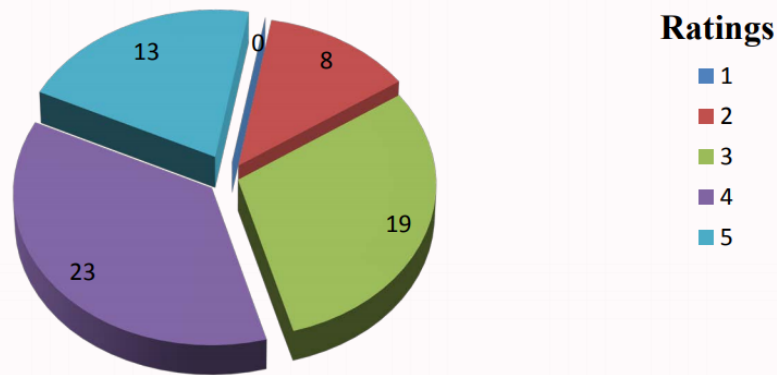


### P65 -- Right to Access

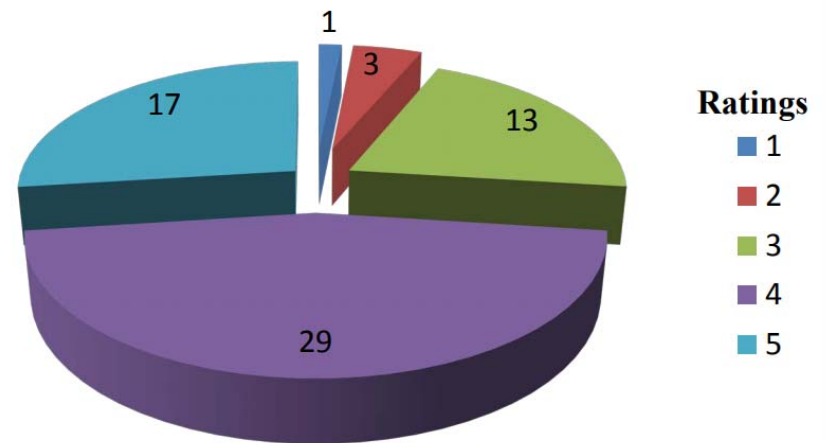


# Risk analysis and risk management

**S 2 Security Risk Analysis Ratings**  
63 Covered Entities



**S 3 Risk Management Ratings**



**Not easy to get right, apparently....**

# HIPAA audits

- "What is coming after phase two audit?" the audience member then asked. "That is a very good question. I know the goals are for on-site audits. I believe that is what will come next."  
--Linda Sanches, OCR Senior Advisor

# Don't forget the Security Rule

- OBTAIN and READ the HIPAA Security Rule.
- You can find it at 45 C.F.R. Part 164, Subpart C  
(<https://www.gpo.gov/fdsys/pkg/CFR-2007-title45-vol1/pdf/CFR-2007-title45-vol1-part164-subpartC.pdf>)
- OCR webpage for Security Rule text and resources:

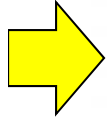
<http://www.hhs.gov/hipaa/for-professionals/security/>

# The HIPAA Security Rule



## Security Standards Matrix (Appendix A of the Security Rule)

ADMINISTRATIVE SAFEGUARDS			
Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Security Management Process	§ 164.308(a)(1)	Risk Analysis	(R)
		Risk Management	(R)
		Sanction Policy	(R)
		Information System Activity Review	(R)
Assigned Security Responsibility	§ 164.308(a)(2)		
Workforce Security	§ 164.308(a)(3)	Authorization and/or Supervision	(A)
		Workforce Clearance Procedure	(A)
		Termination Procedures	(A)
Information Access Management	§ 164.308(a)(4)	Isolating Health Care Clearinghouse Functions	(R)
		Access Authorization	(A)
		Access Establishment and Modification	(A)
Security Awareness and Training	§ 164.308(a)(5)	Security Reminders	(A)
		Protection from Malicious Software	(A)
		Log-in Monitoring	(A)
		Password Management	(A)
Security Incident Procedures	§ 164.308(a)(6)	Response and Reporting	(R)
Contingency Plan	§ 164.308(a)(7)	Data Backup Plan	(R)
		Disaster Recovery Plan	(R)
		Emergency Mode Operation Plan	(R)
		Testing and Revision Procedures	(A)
		Applications and Data Criticality Analysis	(A)
Evaluation	§ 164.308(a)(8)		
Business Associate Contracts and Other Arrangements	§ 164.308(b)(1)	Written Contract or Other Arrangement	(R)



PHYSICAL SAFEGUARDS			
Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Facility Access Controls	§ 164.310(a)(1)	Contingency Operations	(A)
		Facility Security Plan	(A)
		Access Control and Validation Procedures	(A)
		Maintenance Records	(A)
Workstation Use	§ 164.310(b)		
Workstation Security	§ 164.310(c)		
Device and Media Controls	§ 164.310(d)(1)	Disposal	(R)
		Media Re-use	(R)
		Accountability	(A)
		Data Backup and Storage	(A)
TECHNICAL SAFEGUARDS			
Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Access Control	§ 164.312(a)(1)	Unique User Identification	(R)
		Emergency Access Procedure	(R)
		Automatic Logoff	(A)
		Encryption and Decryption	(A)
Audit Controls	§ 164.312(b)		
Integrity	§ 164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	(A)
Person or Entity Authentication	§ 164.312(d)		
Transmission Security	§ 164.312(e)(1)	Integrity Controls	(A)
		Encryption	(A)
ORGANIZATIONAL REQUIREMENTS			
Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Business associate contracts or other arrangements	§ 164.314(a)(1)	Business Associate Contracts	(R)
		Other Arrangements	(R)
Requirements for Group Health Plans	§ 164.314(b)(1)	Implementation Specifications	(R)
POLICIES AND PROCEDURES AND DOCUMENTATION REQUIREMENTS			
Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Policies and Procedures	§ 164.316(a)		
Documentation	§ 164.316(b)(1)	Time Limit	(R)
		Availability	(R)
		Updates	(R)



CENTERS for MEDICARE & MEDICAID SERVICES

Volume 2 / Paper 6

18

6/2005; rev. 3/2007

**Fredrikson**  
& BYRON, P.A.



# Disclaimers and notes

- You need a technical expert.
- The Security Rule Analysis is organization specific. You will have to do some work after this presentation.
- The Security Rule Analysis is a ongoing process.
- HIPAA does not require that an independent expert conduct your Security Risk Analysis.
- Be skeptical of certifications. Probe the content. Look for substance.

# 45 C.F.R. 164.308(a)(1)(i)-(ii)(A),(B)

- **Establish and maintain a Security management process.**

Implement policies and procedures to prevent, detect, contain, and correct security violations.

- **Implementation specifications:**

- ✓ **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.

- ✓ **Risk management (Required).** Implement **security measures** sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level

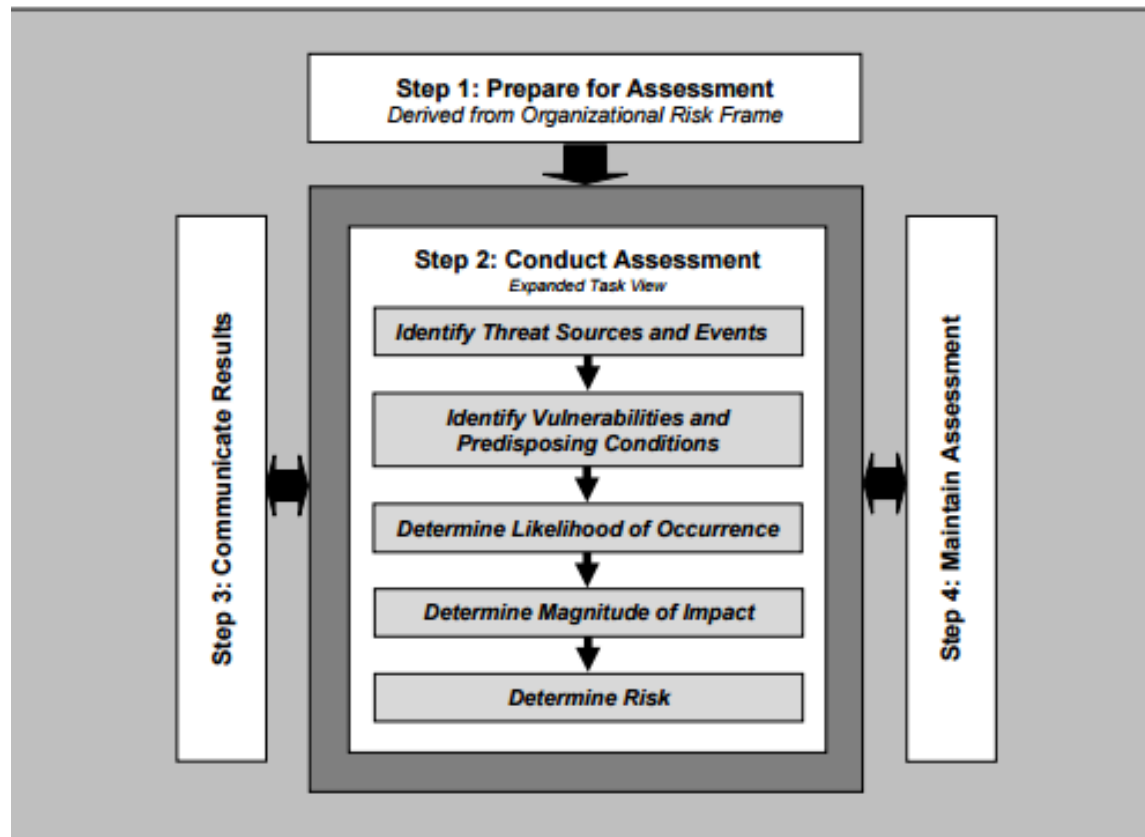


Figure 5: Risk Assessment Process,  
<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>, accessed 11-13-2016.

# NIST Guidance

- There is a lot. See <http://www.hhs.gov/hipaa/for-professionals/security/guidance/> for NIST guidance handpicked by OCR.
- This is the best overall NIST guidance document for performing a Security Risk Analysis:  
<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>

# Step 1: Prepare for the assessment

- Who?
  - Security Officer
  - Director of Operations?
  - IT personnel, consultant
  - Note taker
- When?
  - 2006

# Step 2: Conduct assessment

- Use a chart form – Excel spreadsheet
- ROWS – One row for each location where PHI (including ePHI) resides in your organization. This is called your asset inventory.

*EXAMPLES (THIS IS NOT AN EXHAUSTIVE LIST):*

Desktops, laptops, mobile devices, copy machines, shredding bins, physical servers, cloud servers, web-based email system, employee offices, workstations, shredding bins, recycling bins, VENDORS who touch PHI, . . . .

Don't forget to consider each business location.

# Conduct assessment (cont.)

- COLUMNS – One column for each of the following:
  - Threat
  - Likelihood of event
  - Magnitude of impact
  - Level of risk
  - Security measures in place
  - Security measures needed
  - Timeline for future implementation measure

*NON-EXHAUSTIVE EXAMPLE ONLY – INVENTORY OF ASSETS WILL VARY BY ORGANIZATION*

Inventory of PHI	Threats (Threat-source, vulnerability)	Likelihood of event	Magnitude of impact	Level of risk	Security measures in place	Security measures needed	Timeline for implementing future measures
Desktop computers							
Network							
Cloud server							
Copy machines							
Employee smartphones							



# Threats

- A threat is a potential for a particular threat-source to successfully exercise a particular vulnerability.
- A vulnerability is a weakness that can be accidentally triggered or intentionally exploited.
- May group threats into general categories (e.g., natural, human, environmental).

# Examples of threats, groups of threats

- Theft
- Loss
- Malware
- Snooping employee
- Sending PHI to wrong recipient
- Natural disaster

# Likelihood of an event

- “The term likelihood . . . is not likelihood in the strict sense of the term; rather, it is a likelihood score. Risk assessors do not define a likelihood function in the statistical sense. Instead, risk assessors assign a score (or likelihood assessment) based on available evidence, experience, and expert judgment.”
  - <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>
- Very low, low, moderate, high, very high

# Magnitude of impact

- “An organization must assess the magnitude of the potential impact resulting from a threat triggering or exploiting a specific vulnerability. An entity may use either a qualitative or quantitative method or a combination of the two methods to measure the impact on the organization.”
  - <http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf>
- Very low, low, moderate, high, very high

# Level of risk

- “Organizations should assign risk levels for all threat and vulnerability combinations identified during the risk analysis. The level of risk could be determined, for example, by analyzing the values assigned to the likelihood of threat occurrence and resulting impact of threat occurrence. The risk level determination might be performed by assigning a risk level based on the average of the assigned likelihood and impact levels.”
  - <http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf>

**TABLE I-2: ASSESSMENT SCALE – LEVEL OF RISK (COMBINATION OF LIKELIHOOD AND IMPACT)**

<b>Likelihood</b> (Threat Event Occurs and Results in Adverse Impact)	<b>Level of Impact</b>				
	<b>Very Low</b>	<b>Low</b>	<b>Moderate</b>	<b>High</b>	<b>Very High</b>
<b>Very High</b>	Very Low	Low	Moderate	High	Very High
<b>High</b>	Very Low	Low	Moderate	High	Very High
<b>Moderate</b>	Very Low	Low	Moderate	Moderate	High
<b>Low</b>	Very Low	Low	Low	Low	Moderate
<b>Very Low</b>	Very Low	Very Low	Very Low	Low	Low

<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>

# Security measures in place

- Encryption
- Firewall
- Training
- Audit access log
- Lock and key
- Vendor due diligence

# Security measures needed

- “Once risk is identified and assigned a risk level, the covered entity should begin to identify the actions required to manage the risk. The purpose of this step is to begin identifying security measures that can be used to reduce risk **to a reasonable and appropriate level**. When identifying security measures that can be used, it is important to **consider factors such as: the effectiveness of the security measure; legislative or regulatory requirements that require certain security measures to be implemented; and requirements of the organization’s policies and procedures**. Any potential security measures that can be used to reduce risks to EPHI should be included in documentation.”

HIPAA Security Series 6

<http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf>



# Layers of Security



©2015 Aris Medical Solutions. All rights reserved

**Fredrikson**  
& BYRON, P.A.

# Timeline for implementing future measures

- You must have a plan for implementing future measures – this is the “risk management” part of 45 C.F.R 164.308(a).

*NON-EXHAUSTIVE, EXAMPLE ONLY – RISK ANALYSIS WILL VARY BY ORGANIZATION*

Inventory of PHI	Threats (Threat-source, vulnerability)	Likelihood of event	Magnitude of impact	Level of risk	Security measures in place	Security measures needed	Timeline for implementing future measures
Laptops	<b>1. Theft</b>	Moderate	Very high	Very high	Password-protected, encrypted hard drive, lockable carrier	Automatic, timed logoff  Policy on taking laptops off-site  Education and training	End of Q4 2016  End of Q4 2016  End of Q1 2017

# Step 3: Communicate results

- The Security Rule Analysis exercise is actually supposed to help you.
- Notify responsible parties of their duties to implement certain measures.
- Train all members of the workforce on Security Rule policies and procedures. THIS IS REQUIRED BY THE REGULATION.
- DOCUMENT and DATE all analysis, communication, and training efforts.

# Step 4: Maintain assessment

- You must conduct the Security Rule Analysis steps
  - MORE THAN ONCE. Periodically. Preferably every six months.

AND



- EVERY TIME THERE IS A NEW SOURCE/LOCATION OF PHI IN YOUR ORGANIZATION.
  - E.g., you add a new electronic tool for documenting cares.
  - E.g., you engage a new cloud vendor.

# Dinged for no Security Risk Analysis

- Anchorage Community Mental Health Services paid \$150,000 and adopted a corrective action plan after a breach of unsecured ePHI caused by a malware incident affected 2,743 individuals. The investigation revealed ACMHS had adopted sample Security Rule policies and procedures in 2005, but these were not followed. Moreover, the security incident was the direct result of ACMHS failing to identify and address basic risks, such as not regularly updating their IT resources with available patches and running outdated, unsupported software.

# Things are a little uncertain....

## Secretary of HHS:

Tom Price (Feb. 10 - Sept. 29)  Don J. Wright (for 12 days)  Eric Hargan (new acting Sec)

## OCR:

Roger Severino still in charge at OCR, no clear signals about priorities for privacy matters

- Still, a few compliance updates....

# HIPAA and the Opioid Crisis

- October 27: OCR released new guidance on sharing PHI with family members, friends, and legal personal representatives when a patient may be in crisis and incapacitated, such as during an opioid overdose.
- Followed President Trump's declaration of a nationwide public health emergency.



## How HIPAA<sup>1</sup> Allows Doctors to Respond to the Opioid Crisis



**HIPAA regulations allow health professionals to share health information with a patient's loved ones in emergency or dangerous situations** – but misunderstandings to the contrary persist and create obstacles to family support that is crucial to the proper care and treatment of people experiencing a crisis situation, such as an opioid overdose. This document explains how health care providers have broad ability to share health information with patients' family members during certain crisis situations



# Disclosures to Family, Friends

- HIPAA permits providers to share information without permission:
  - If the provider determines that doing so is in the best interests of an **incapacitated or unconscious** patient and the information shared is directly related to the family or friend's involvement in the patient's health care or payment of care (e.g., talking to the patient's parents about an overdose and related medical information, but not sharing medical information unrelated to the overdose without permission).
  - Informing persons in a position to prevent or lessen a **serious and imminent threat to a patient's health or safety** (e.g., informing family, friends, or caregivers of the opioid abuse after determining that the patient poses a serious and imminent threat to his or her health through continued opioid abuse upon discharge).

# Disclosures to Family, Friends

- For patients with decision-making capacity: must provide an opportunity to agree or object, *unless* there is a serious and imminent threat of harm to health.
- A patient's decision-making capacity may change during the course of treatment.
- HIPAA recognizes patient's personal representatives according to state law.

# What about Part 2?

<sup>2</sup> This guidance does not discuss the requirements of other federal or state laws that apply to individuals' health information, including the federal regulations that provide more stringent protections for the confidentiality of substance use disorder patient records maintained in connection with certain federally assisted substance use disorder treatment programs (42 CFR Part 2 implementing 42 U.S.C. §290dd-2). HIPAA does not interfere with other laws or medical ethics rules that are more protective of patient privacy.

# What about Part 2?

- Part 2 restrictions apply to:
  - “Programs”:
    - An individual or entity (other than a general medical facility) who holds itself out as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment; or
    - An identified unit within a general medical facility that holds itself out as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment; or
    - Medical personnel or other staff in a general medical facility whose primary function is the provision of substance use disorder diagnosis, treatment, or referral for treatment and who are identified as such providers.
  - Individuals or entities who receive patient records directly from a part 2 program or other lawful holder of patient identifying information and who are notified of the prohibition on re-disclosure in accordance with Part 2.

# Medical Emergencies

- *General rule.* Under the procedures required by paragraph (c) of this section, patient identifying information may be disclosed **to medical personnel** to the extent necessary to meet a bona fide medical emergency in which the patient's prior informed consent cannot be obtained.

# HIPAA and Emergencies

- Limited Waivers of HIPAA Sanctions
  - If the President declares an emergency or disaster *and* the Secretary of HHS declares a public health emergency, the Secretary may waive sanctions and penalties against a covered entity that does not comply with certain provisions of the Privacy Rule.
  - The Privacy Rule remains in effect.
  - The waivers are limited and apply only for limited periods of time.

# HIPAA and Emergencies

- **Waivers:**
  - Prior to 2017, most recent was Hurricane Katrina.
  - Bulletins issued in 2017 for the following natural disasters:
    - California Wildfires (October 2017)
    - Hurricane Maria (September 2017)
    - Hurricane Irma (September 2017)
    - Hurricane Harvey (August 2017)

# HIPAA and Emergencies

- Oct. 3: Clarification regarding disclosures to friends and family for notification purposes
  - Response to Las Vegas mass shooting.
  - Only a clarification, no new law.
- HIPAA allows CEs to share PHI with those involved in a patient's care, and as necessary to “identify, locate, share general condition/death.”
  - Can include notification of family, police, press, or even public at large.



# Medical device info sharing

- FDA guidance on information sharing
  - Clarified that manufacturers may share information from medical devices with patients, upon patient request
  - Draft document June 10, 2016; final issued Oct. 30, 2017
  - Specifically says that it does not affect HIPAA

# Patient access and charging for copies

- Guidance published middle of 2016, but still lots of questions/confusion
- Generally patients have right of access to their own PHI/designated record set
  - Medical records, billing records, and other records used by/for the CE to make decisions about individuals (ANY individuals)
    - Maybe not QA/QI, business planning, patient safety activity records
    - Not psychotherapy notes or info compiled for use in legal proceeding

## Problem area: Patient access

- Personal representatives can get PHI
- May require request for access to be in writing
  - Should NOT require an authorization
  - May require use of specific form, if it doesn't create a barrier or unreasonable delay
- May request that information go to another person designated by the individual

# Patient access

- Provide in the form/format requested (if readily producible), or readable hard copy form
- Provide in the manner requested
  - Includes arranging a convenient time for pick up, or having a copy mailed or emailed
  - Not required to take on unacceptable levels of risk to accommodate
  - Mail and email generally considered “readily producible” by all covered entities
  - Can’t require someone to come in to pick up copies

# Fees for copies

- “Reasonable, cost-based fee”
- ONLY cost of:
  - Labor for **copying** (paper or electronic)
  - Supplies for creating the paper copy/electronic media
  - Postage (when mailing)
  - Labor to prep summary/explanation (if agreed to by individual in advance, including fees)
- Not supposed to be a revenue stream
- Must inform of cost in advance of approximate fee\*

# Fees for copies—three options

- Actual costs
  - Still have to notify individuals in advance of the approximate fee
- Average costs
  - Can develop a schedule of costs for labor based on average labor costs to fulfill standard types of access requests.
  - Can add any applicable supply/postage costs
  - Can be calculated/charged as a per-page fee only when in paper form
- Flat fee for electronic copies maintained electronically
  - \$6.50
  - Includes labor, supplies and postage

# Fees for copies

- Still pay attention to state laws that provide more access
  - Some allow individuals to get a free copy—that still applies
  - State laws with higher permitted charges are overridden by HIPAA

# Privacy Officer Woes

- Training
  - How often?
  - What form?
  - Vendors?



# Privacy Officer Woes

- Breaches
  - What is a breach?
  - When must I report a breach?

# Privacy Officer Woes

- BAAs

# Questions?



Briar Andresen  
Fredrikson & Byron, P.A.  
612.492.7057  
bandresen@fredlaw.com



Katie Ilten  
Fredrikson & Byron, P.A.  
612.492.7428  
kilten@fredlaw.com



Marguerite Ahmann  
Fredrikson & Byron, P.A.  
612.492.7495  
mahmann@fredlaw.com