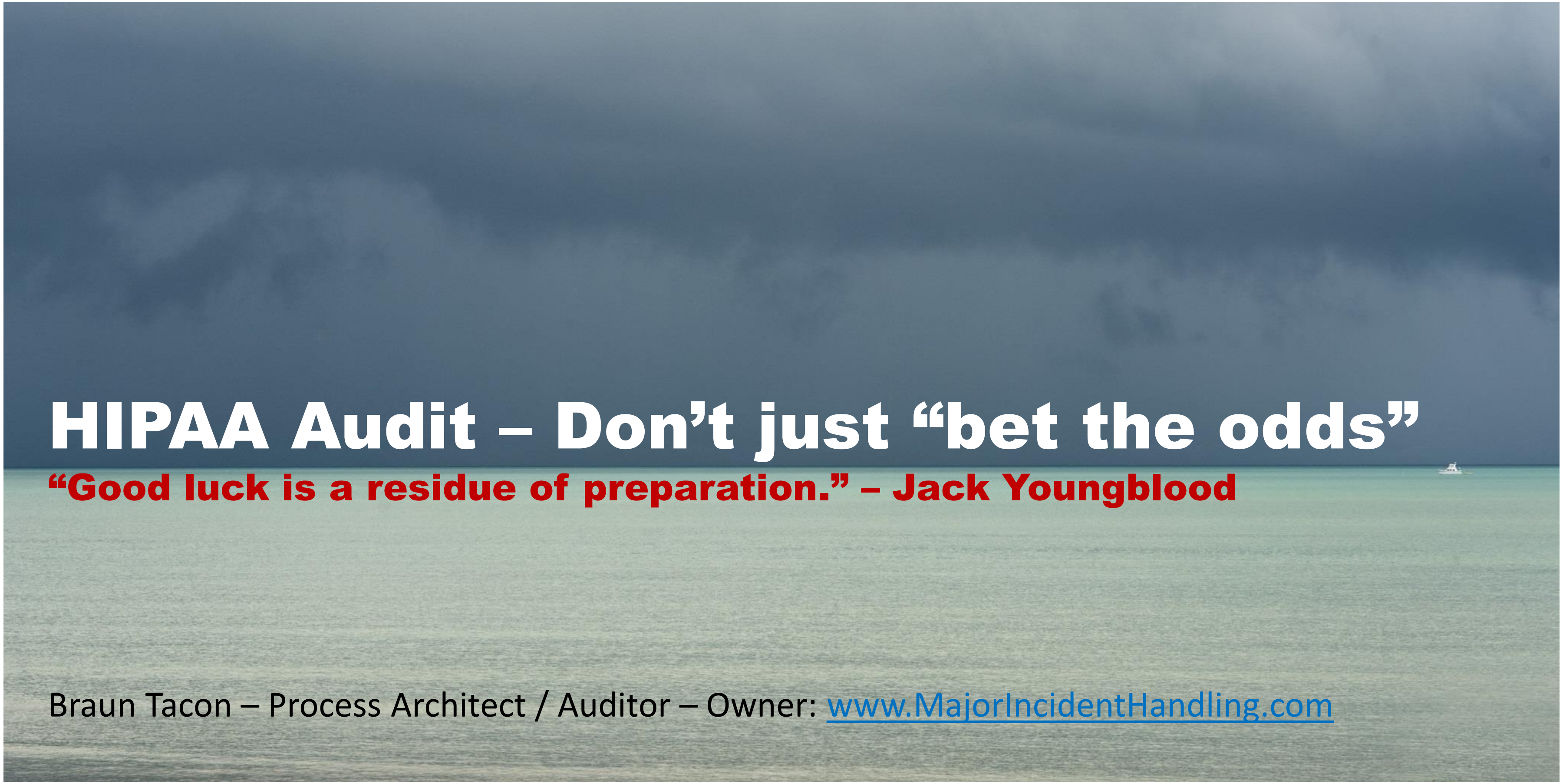


HIPAA Audit – Don’t just “bet the odds”

“Good luck is a residue of preparation.” – Jack Youngblood

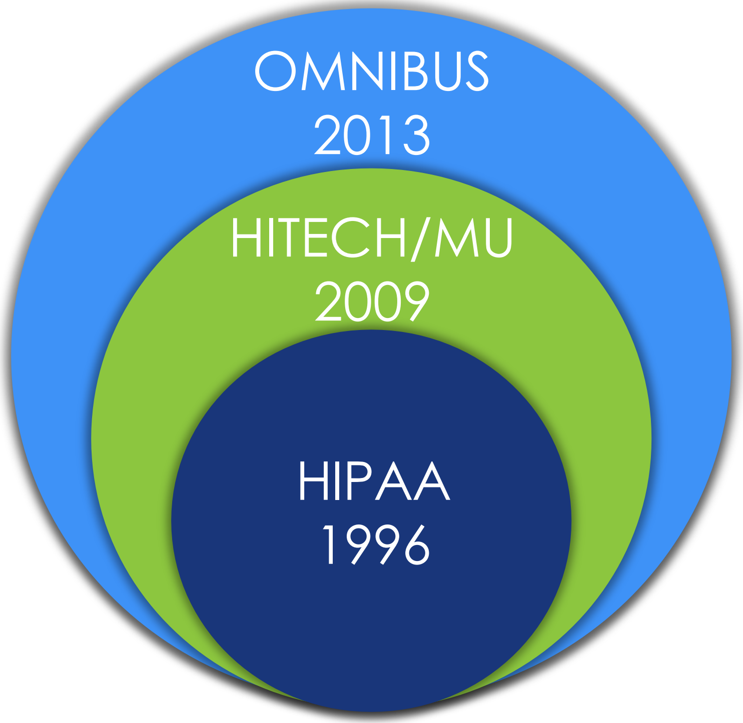
Braun Tacon – Process Architect / Auditor – Owner: www.MajorIncidentHandling.com

Random odds ….

- Winning Lotto……………………………………………………………………….1 in 175 Million
- Attacked by a shark……………………………………………………………..1 in 11.5 Million
- Hit by Lightning…………………………………………………………………..1 in 960,000
- Hole in One………………………………………………………………………..1 in 12,500
- **Random HIPAA Audit………………………………………………………….1 in 10,000**
- **Meaningful use Audit………………………………………………………..1 in 10**
- **Breach-Related Audit……………………………………………….………..1 in ?**

HIPAA At A Glance

- **HIPAA – Aug 1996**
  - Provide for HCI portability between jobs while furthering innovation and patient care
- Privacy Rule published Dec 2000 & Aug 2002
- Security Rule published Feb 2003
- Enforcement Rule final – Feb 2006
- **HITECH / Meaningful Use (MU) – Feb 2009**
  - Incentivize use of EMRS through cash payments
  - Added BA's and Third Parties to the RACI list
  - Introduced the Breach Notification Rule
- **Omnibus – Jan 2013**
  - Dot the I's, Cross the T's, Tie it all together
  - Emphasis on increased enforcement / fines
- **Corrective Actions and / or Fines – Ongoing**



Enforcement Accelerating in 2016 and Beyond

Some 2016 Enforcement Examples

Entity	Financial Penalty
Feinstein Institute for Medical Research	$3.9 Million
University of Mississippi Medical Center	$2.75 Million
Oregon Health & Science University	$2.7 Million
New York Presbyterian	$2.2 Million
North Memorial Health Care	$1.55 Million
Raleigh Orthopaedic Clinic, P.A	$750,000
Catholic Health Care Services of the Archdiocese of Philadelphia	$650,000
Lincare, Inc.	$239,800
Complete P.T., Pool & Land Physical Therapy	$25,000

Source: U.S. Department of Health and Human Services

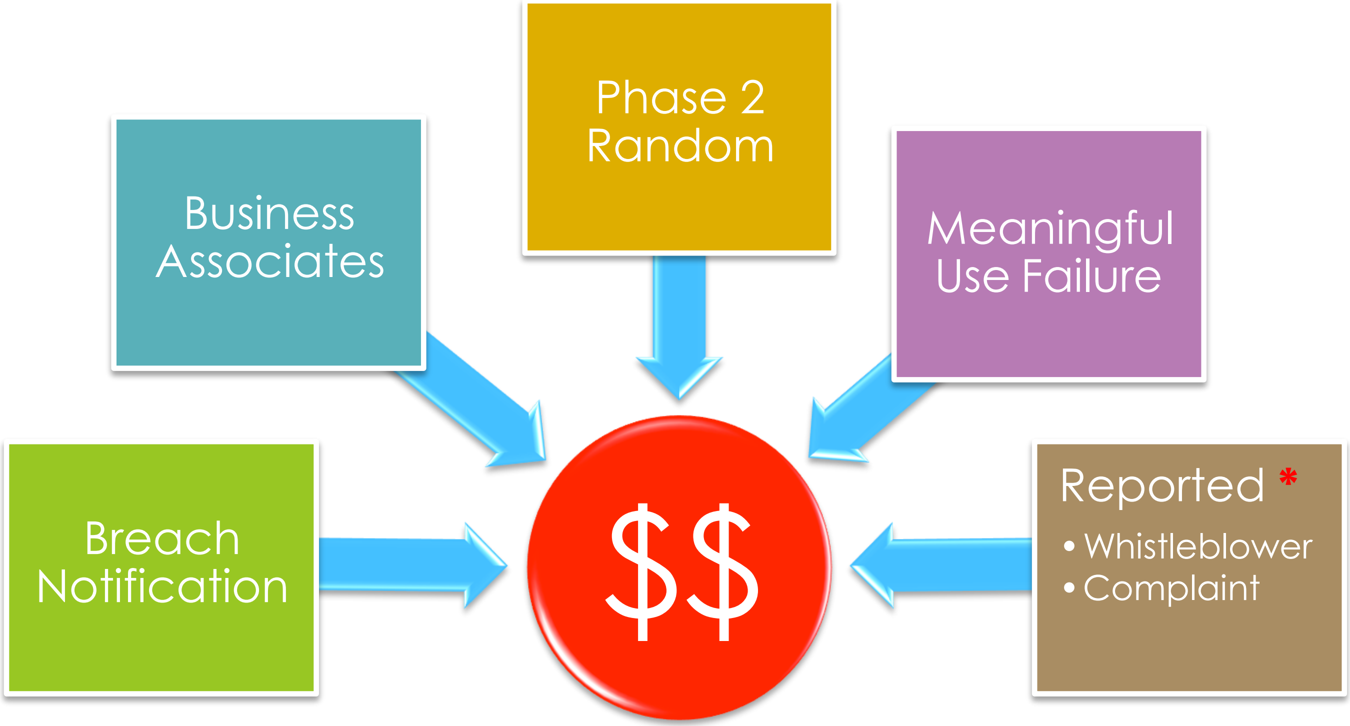
- OCR has investigated and resolved over 24,617 cases by requiring changes in privacy practices and corrective actions

- OCR has investigated complaints against many different types of entities including: national pharmacy chains, major medical centers, group health plans, hospital chains, skilled nursing facilities and small provider offices

- **Since OCR's first resolution agreement in 2008, to date (November 2016), OCR has settled 41 such cases resulting in a total dollar amount of $48,679,700.00.**

Source: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html

Threat Vectors For A HIPAA Audit



Business Associates

Phase 2 Random

Meaningful Use Failure

Breach Notification

$$

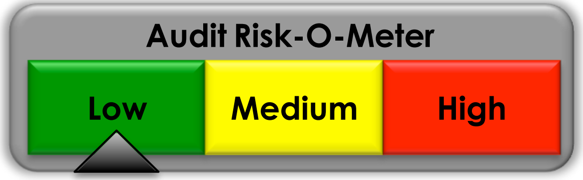
Reported *

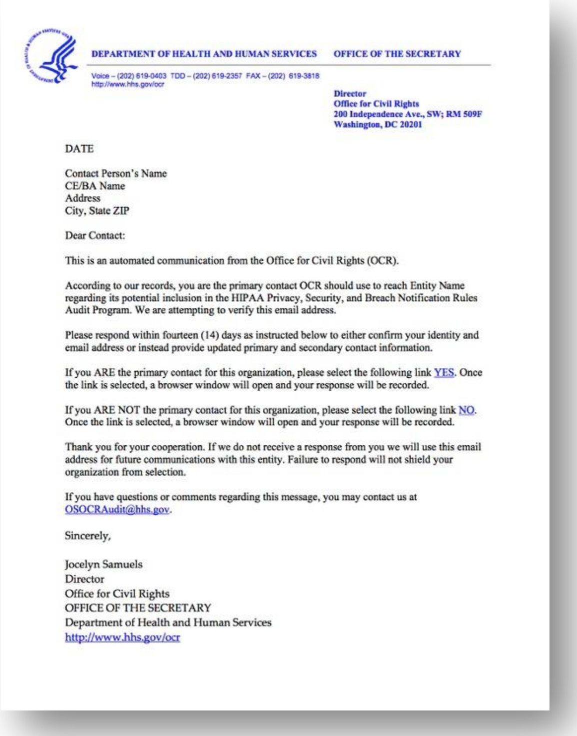
- Whistleblower
- Complaint

* HHS is REQUIRED by law to investigate ALL HIPAA violation complaints

Phase 2 Random Audits

- Covered Entities and Business Associates will be randomly audited
- Began: March 22, 2016
- Business Associates sometime late 2016
- Will not end. Enforcement is accelerating





DEPARTMENT OF HEALTH AND HUMAN SERVICES OFFICE OF THE SECRETARY

Voice – (202) 619-0403 TDD – (202) 619-2357 FAX – (202) 619-3818
http://www.hhs.gov/ocr

Director
Office for Civil Rights
200 Independence Ave., SW; RM 509F
Washington, DC 20201

DATE

Contact Person's Name
CE/BA Name
Address
City, State ZIP

Dear Contact:

This is an automated communication from the Office for Civil Rights (OCR).

According to our records, you are the primary contact OCR should use to reach Entity Name regarding its potential inclusion in the HIPAA Privacy, Security, and Breach Notification Rules Audit Program. We are attempting to verify this email address.

Please respond within fourteen (14) days as instructed below to either confirm your identity and email address or instead provide updated primary and secondary contact information.

If you ARE the primary contact for this organization, please select the following link YES. Once the link is selected, a browser window will open and your response will be recorded.

If you ARE NOT the primary contact for this organization, please select the following link NO. Once the link is selected, a browser window will open and your response will be recorded.

Thank you for your cooperation. If we do not receive a response from you we will use this email address for future communications with this entity. Failure to respond will not shield your organization from selection.

If you have questions or comments regarding this message, you may contact us at OSOCRAudit@hhs.gov.

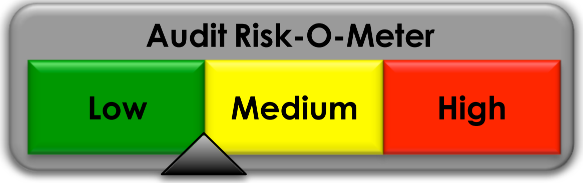
Sincerely,

Jocelyn Samuels
Director
Office for Civil Rights
OFFICE OF THE SECRETARY
Department of Health and Human Services
http://www.hhs.gov/ocr

Meaningful Use Failure

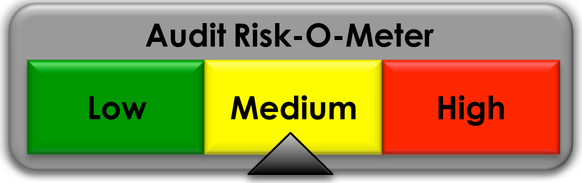
- **5-10%** of providers will be audited by CMS at random

- Having a Security Risk Assessment for Meaningful Use **does not** make you HIPAA Compliant



Complaint or Report Investigations

- Complaint of Security/Privacy violation
  - HHS is REQUIRED by law to investigate ALL HIPAA violation complaints
- Whistleblower
  - Frequently anonymous
  - Sometimes collect a percentage of any money collected



Audit Risk-O-Meter

Low

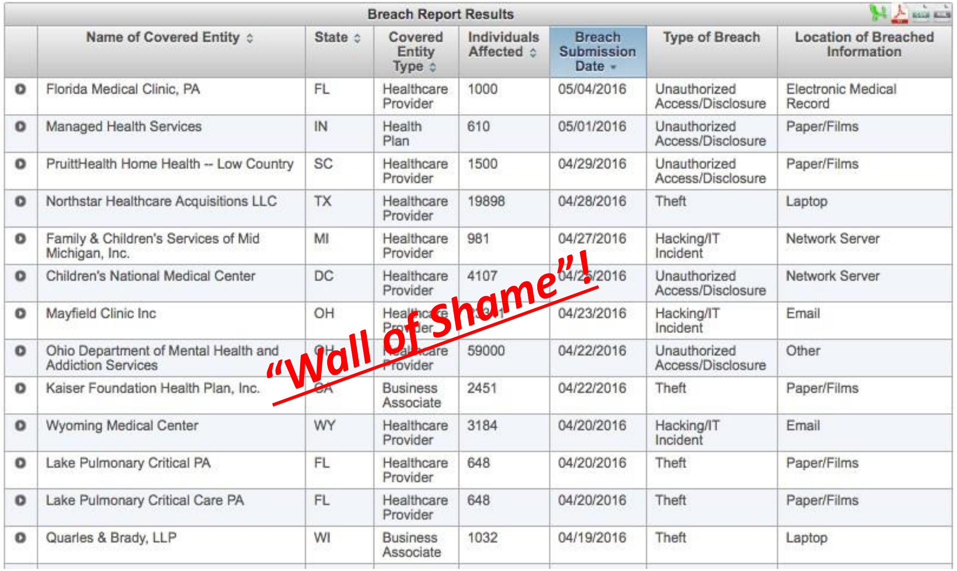
Medium

High

Breach Notification Required

Breach Notification Rule

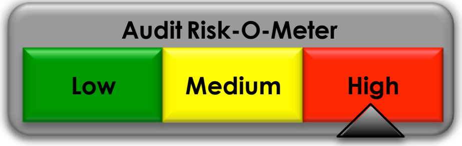
- **Affects < 500 PHI**: must notify all breaches of calendar year by a deadline
- **Affects > 500 PHI**: must notify HHS immediately, publicized in HHS Wall of Shame



Breach Report Results

	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
●	Florida Medical Clinic, PA	FL	Healthcare Provider	1000	05/04/2016	Unauthorized Access/Disclosure	Electronic Medical Record
●	Managed Health Services	IN	Health Plan	610	05/01/2016	Unauthorized Access/Disclosure	Paper/Films
●	PruittHealth Home Health -- Low Country	SC	Healthcare Provider	1500	04/29/2016	Unauthorized Access/Disclosure	Paper/Films
●	Northstar Healthcare Acquisitions LLC	TX	Healthcare Provider	19898	04/28/2016	Theft	Laptop
●	Family & Children's Services of Mid Michigan, Inc.	MI	Healthcare Provider	981	04/27/2016	Hacking/IT Incident	Network Server
●	Children's National Medical Center	DC	Healthcare Provider	4107	04/25/2016	Unauthorized Access/Disclosure	Network Server
●	Mayfield Clinic Inc	OH	Healthcare Provider	23341	04/23/2016	Hacking/IT Incident	Email
●	Ohio Department of Mental Health and Addiction Services	OH	Healthcare Provider	59000	04/22/2016	Unauthorized Access/Disclosure	Other
●	Kaiser Foundation Health Plan, Inc.	CA	Business Associate	2451	04/22/2016	Theft	Paper/Films
●	Wyoming Medical Center	WY	Healthcare Provider	3184	04/20/2016	Hacking/IT Incident	Email
●	Lake Pulmonary Critical PA	FL	Healthcare Provider	648	04/20/2016	Theft	Paper/Films
●	Lake Pulmonary Critical Care PA	FL	Healthcare Provider	648	04/20/2016	Theft	Paper/Films
●	Quarles & Brady, LLP	WI	Business Associate	1032	04/19/2016	Theft	Laptop

"Wall of Shame"!



Full Year Breach Statistics 2016 / 2015

Largest Healthcare Breaches of 2016			
Rank	Entity Type	Cause of Breach	Records Exposed
1	Healthcare Provider	Hacking/IT Incident	3620000
2	Business Associate	Hacking/IT Incident	3466120
3	Healthcare Provider	Hacking/IT Incident	2213597
4	Healthcare Provider	Hacking/IT Incident	882590
5	Healthcare Provider	Hacking/IT Incident	749017
6	Healthcare Provider	Unauthorized Access/Disclosure	651971
7	Healthcare Provider	Hacking/IT Incident	531000
8	Healthcare Provider	Loss	483063
9	Healthcare Provider	Theft	400000
10	Health Plan	Hacking/IT Incident	381504
11	Healthcare Provider	Hacking/IT Incident	300000
12	Healthcare Provider	Theft	205748
13	Healthcare Provider	Unauthorized Access/Disclosure	201000
14	Healthcare Provider	Improper Disposal	113528

2016 Healthcare Data Breaches of 500 or More Records		
Year	# of Breaches (500+)	# of of Records Exposed
2016	324	16,586,112
2015	270	113,267,174

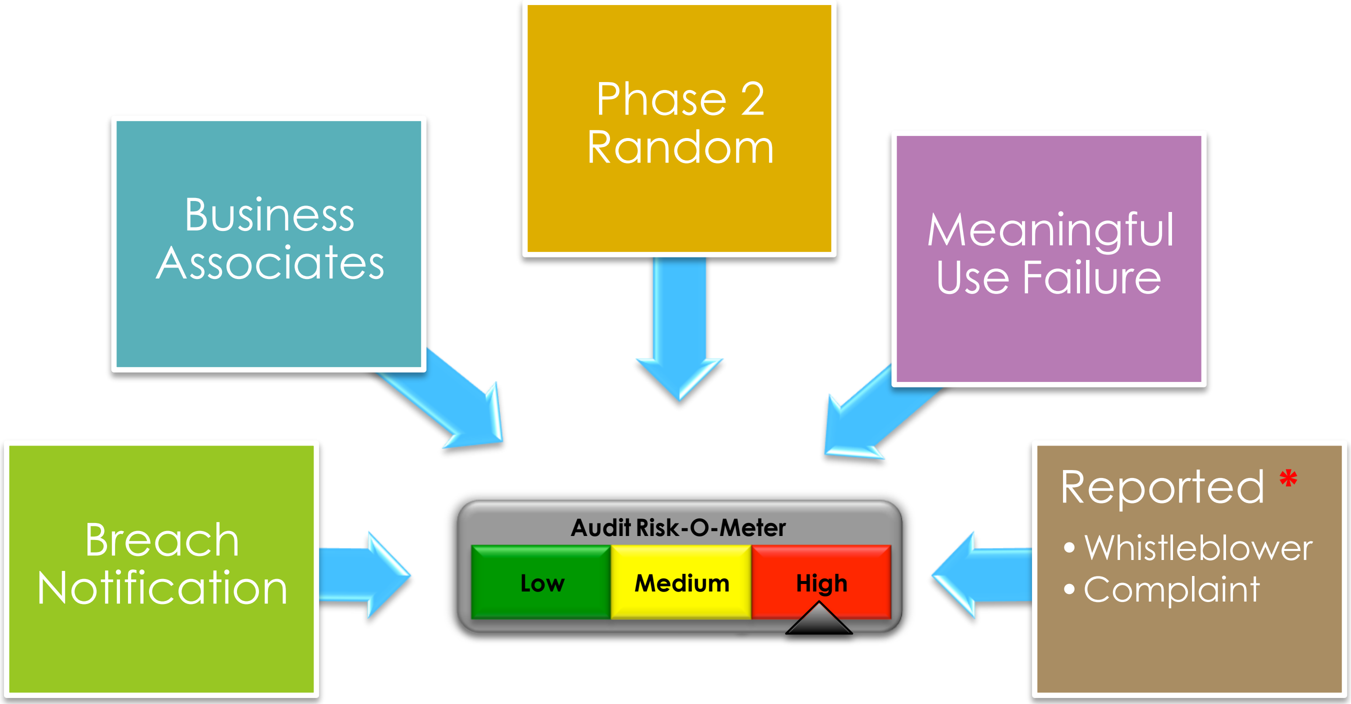
Breaches of More Than 500 Records				
Year	500 to 1000	1,000 to 10,000	10k to 100k	100,001+
2016	88	157	64	14
2015	76	142	37	12

Main Cause of Breach	2016	2015
Unauthorized Access/Disclosure	130	102
Hacking/IT Incident	108	57
Theft	62	81
Loss	16	23
Improper Disposal	7	6

- 2015: Majority of 500+ Breaches due to Device Theft
- **2016: Majority of 500+ Breaches due to Hacking Etc.**
- **Hacking and the theft / loss of IT devices will continue to challenge providers who do not fully appreciate the huge risks of poorly secured IT Networks and unencrypted devices that are supporting EMRs & ePHI**

Source: http://www.hipaajournal.com/largest-healthcare-data-breaches-of-2016-8631/

So I’m Getting Audited – What’s Next?



Business Associates

Phase 2 Random

Meaningful Use Failure

Breach Notification

Audit Risk-O-Meter

Low

Medium

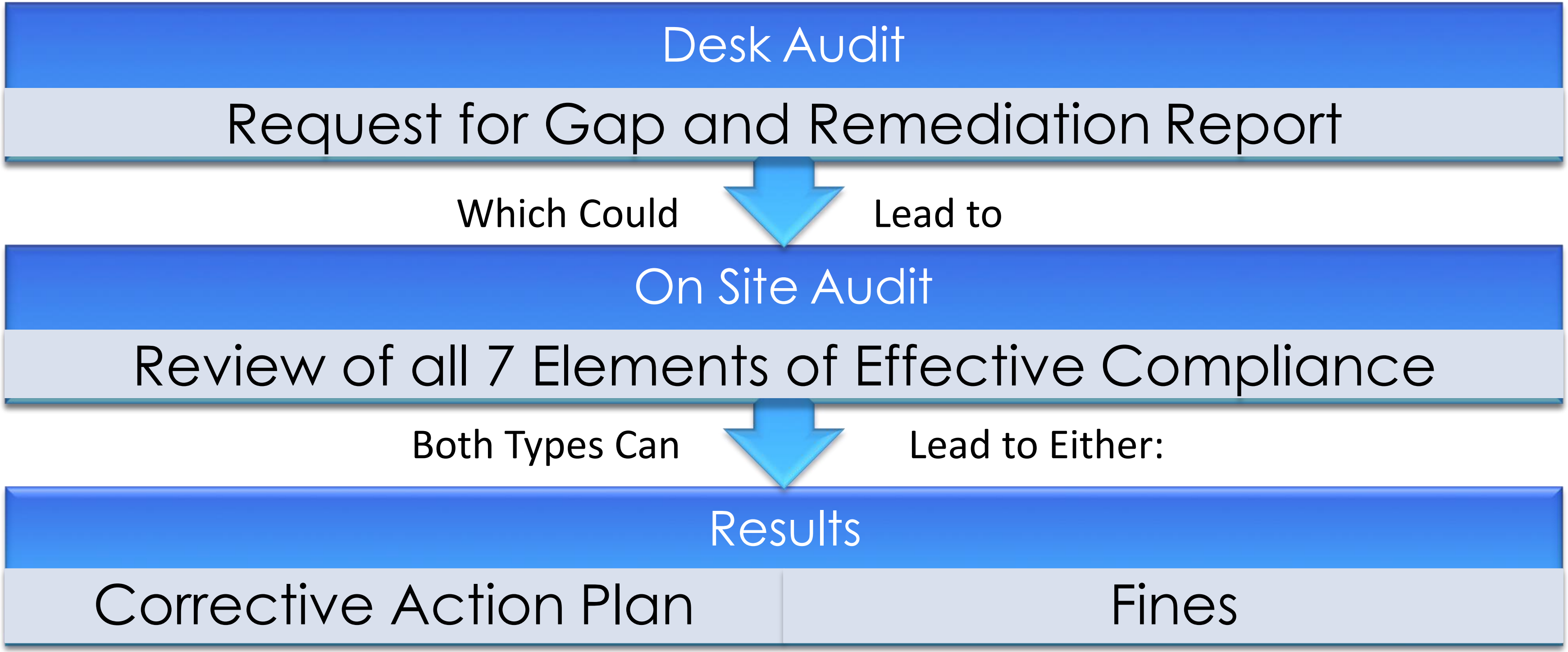
High

Reported *

- Whistleblower
- Complaint

* HHS is REQUIRED by law to investigate ALL HIPAA violation complaints

What to Expect if You Get Audited



Desk Audit

Request for Gap and Remediation Report

Which Could Lead to

On Site Audit

Review of all 7 Elements of Effective Compliance

Both Types Can Lead to Either:

Results

Corrective Action Plan

Fines

OR BOTH

Audit Outcome – Malware Infection (Hacking)

- Who: University of Massachusetts Amherst (UMass)
- What: A **workstation was infected with malware** (virus) that may have led to the release of the ePHI of over 1,670 individuals
- Why: A lack of appropriate policies and procedures, inappropriate or missing technical security measures, as well as the absence of **comprehensive risk analysis** all contributed to the OCR Audit and Fine
- Settlement: **$650,000 and CAP (Corrective Action Plan)** (11/6/16)

Source: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/umass

Audit Outcome – Laptop Loss / Theft

- Who: University of Mississippi Medical Center (UMMC)
- What: **Laptop loss / theft**, 10,000 patient records
- Why: A lack of appropriate policies and procedures, failure to implement physical safeguards, failure to assign unique user names and allowing shared access to ePHI all contributed to th OCR Audit and Fine
- Settlement: **$2,750,000 and CAP (Corrective Action Plan)** (7/7/2013)

Source: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/UMMC/index.html

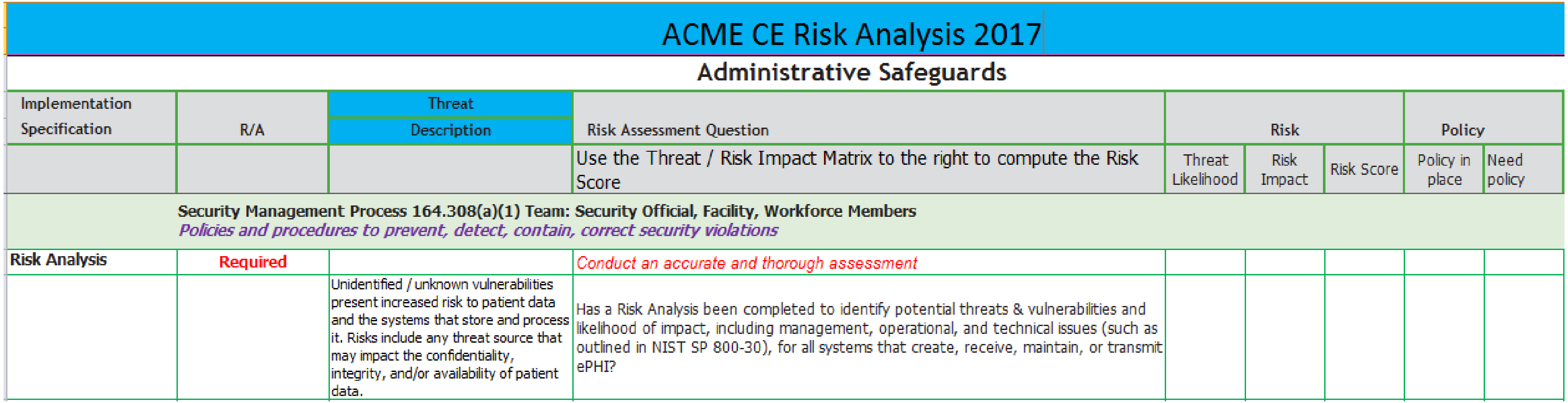
All These Outcomes Sound Bad

- **Yes, many of the potential outcomes are not good**
- **HHS is incented to enforce with prejudice, after an Inspector General (IG) Report called out the HHS for poor enforcement**
- **Expect more "Wall of Shame" type tactics as well as increasing financial penalties in the name of enforcement and PR**
- ***Looks like the odds are against me. What can I do?***

Your Best Defense Is A Good Offense

- Review your current HIPAA risk analysis procedures
- Review your policies and procedures to ensure compliance with all HIPAA Requirements, including those considered "addressable", as well as the recent Breach Notification Rule
- Every portable devices (laptops/smartphone/med-device) that does or can contain PHI must be encrypted by Policy and must be verifiably enforced. Remote wipe is a big plus
- Don't ignore new and significant threats. Do you know what "RansomWare" is? If you don't, you need to find out ASAP

It All Begins With A Risk Analysis



ACME CE Risk Analysis 2017

Administrative Safeguards

Implementation Specification	R/A	Threat Description	Risk Assessment Question	Risk			Policy	
			Use the Threat / Risk Impact Matrix to the right to compute the Risk Score	Threat Likelihood	Risk Impact	Risk Score	Policy in place	Need policy
	Security Management Process 164.308(a)(1) Team: Security Official, Facility, Workforce Members ***Policies and procedures to prevent, detect, contain, correct security violations***							
Risk Analysis	**Required**		*Conduct an accurate and thorough assessment*					
		Unidentified / unknown vulnerabilities present increased risk to patient data and the systems that store and process it. Risks include any threat source that may impact the confidentiality, integrity, and/or availability of patient data.	Has a Risk Analysis been completed to identify potential threats & vulnerabilities and likelihood of impact, including management, operational, and technical issues (such as outlined in NIST SP 800-30), for all systems that create, receive, maintain, or transmit ePHI?					

Have Questions?

Need Help?

Risk Analysis or Assessment?

Business Continuity or Disaster Planning?

info@MajorIncidentHandling.Com