

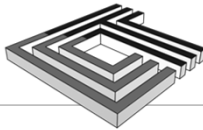
OCR update and Other HIPAA Issues to Keep You Up At Night!

Presented by:

Marti Arvin, JD, CHC-F, CCEP-F, CHRC, CHPC
Vice President of Audit Strategy



CynergisTek was recognized in the 2016 KLAS Security Advisory Services report for having the highest overall client satisfaction, performance and impact on security preparedness in healthcare.




CYNERGISTEK



CynergisTek won the 2017 Best in KLAS award for Cyber Security Advisory Services.

Meeting Agenda



Review Proposal Objectives, Process, Outputs, and Timeline.

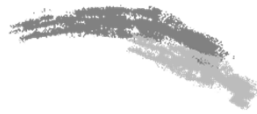
1 OCR update

2 Privacy and Security Vendor Management Risks

3 Compliance and Privacy Key Considerations in Incident Response

4 Questions

OCR UPDATE



OCR Activities

- Proposed policy update
- The changing landscape of data compromises
- The past findings and future process for the audit program

Proposed HIPAA Policy Activity

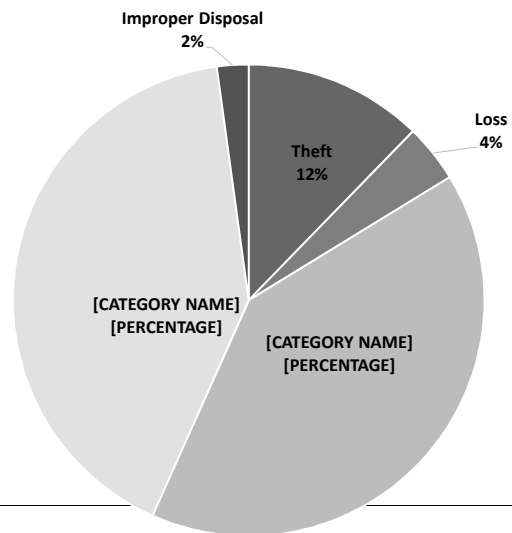
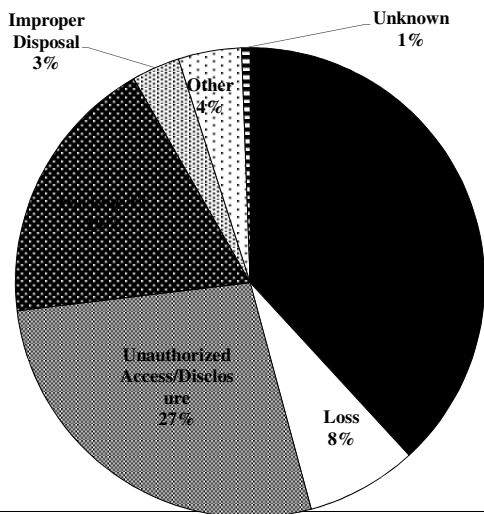
- Notice of Proposed Rulemaking on Good Faith Disclosures by Health Care Providers to Address Opioid Crisis
- Request for Information on Improving Care Coordination and Reducing Regulatory Burden
 - Notice of Privacy Practices
 - Required Provider to Provider Information Sharing
 - Accounting of Disclosures
- Request for Information on Civil Monetary Penalties or Monetary Settlements to Harmed Individuals
- HIPAA/FERPA



500+ Breaches by Type

September 23, 2009 through December 31, 2017

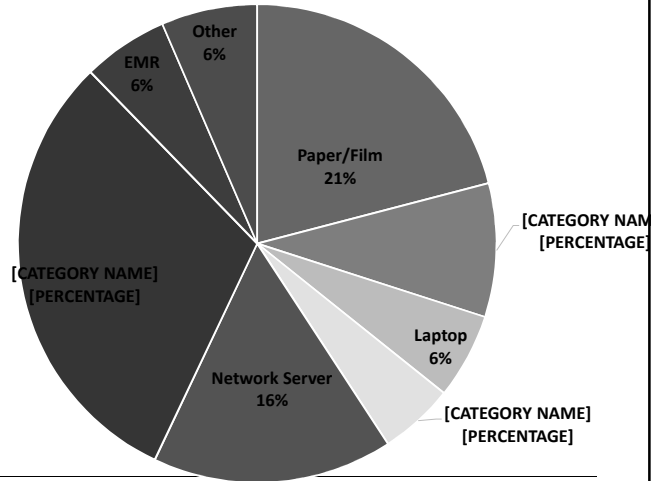
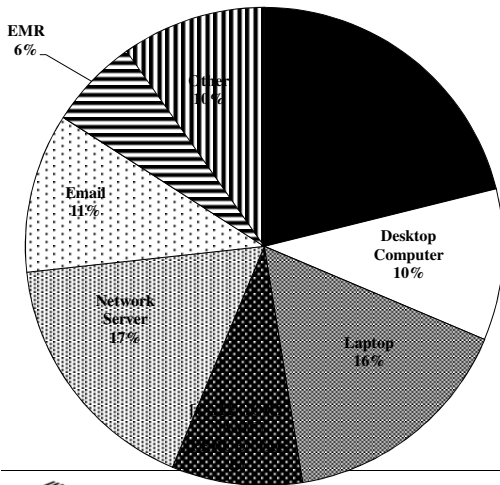
January 1, 2018 through September 30, 2018



500+ Breaches by Location

September 23, 2009 through December 31, 2017

January 1, 2018 through September 30, 2018



7

What Went Wrong

Anthem, Inc. - \$16,000,000

- 78.8m individuals affected
 - Largest health data breach in U.S.
- Gained access through spear fishing in Feb. 2014
- Data extracted from Dec. 2014 to Jan. 2015
 - Included names, addresses, dates of birth, email addresses, SSNs, medical ID numbers and employment information
- Issues with risk analysis, information system activity review, security incident response and reporting, and access controls
- 2 other settlements –
 - National Association of Insurance Commissioners (December 2016)
 - Class Action (August 2018)



8

What went Wrong

ABC Cases \$999,000

- Boston Medical Center - \$100,000
- Brigham and Women's Hospital - \$384,000
- Massachusetts General Hospital - \$515,00
 - BWH and MGH are members of Partners Healthcare - an integrated health care delivery system that includes community hospitals, primary care and specialty physicians, specialty facilities, community health centers and other health-related entities
- All three involved filming for "Save My Life: Boston Trauma"
- Similar to another ABC TV show – "NY Med"
 - "NY Med" resulted in a 2016 settlement with NY Presbyterian for \$2.2m
- OCR Filming Guidance - <https://www.hhs.gov/hipaa/for-professionals/fag/2023/film-and-media/index.html>



AND IT'S NOT JUST HIPAA

- ALL 50 STATES NOW HAVE SOME TYPE OF DATA BREACH NOTIFICATION STATUTE
 - ALABAMA ADDED IN APRIL 2018
 - ALL BUT 8 CONCERN ELECTRONIC DATA ONLY
- IN JUNE, NEW JERSEY AG ANNOUNCED FORMATION OF A NEW DATA PRIVACY & CYBERSECURITY SECTION
- ALSO IN JUNE, THE NEW CALIFORNIA CONSUMER PRIVACY ACT WAS PASSED
- IN SEPTEMBER, THE MASSACHUSETTS AG SIGNED A \$250,000 SETTLEMENT AGREEMENT WITH UMASS MEMORIAL MEDICAL CENTER for a privacy violation
- AND LET'S NOT FORGET ABOUT GDPR!



OCR Audit Findings

- Total covered entities audited: 166
 - 103 for Privacy and Breach Rule compliance
 - 63 for Security Rule compliance
 - Break down of covered entities
 - 9% Health Plans
 - 1% Clearinghouses
 - 90% Providers
- Business associates audited: 41
 - All assessed for Breach Notification and Security Rule compliance

OCR Audit Findings

- OCR comments about the audit process: Under OCR's separate, broad authority to open compliance reviews, OCR could decide to open a separate compliance review in circumstances where significant threats to the privacy and security of PHI are revealed through the audit.

OCR Compliance Rating Scale

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 meets 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 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.

A
↑
↓
F



CEs: Privacy, Security and Breach Notification Rules

Rating at each end of the rankings for all entities (103)		
	5 Rating	1 Rating
Breach Rule		
Timeliness of Notification	15	67
Content of Notification	9	14
Privacy Rule		
Access	11	1
NPP Content	16	2
Electronic NPP	15	59
Security Rule		
Risk Analysis	13	0
Risk Management	17	1



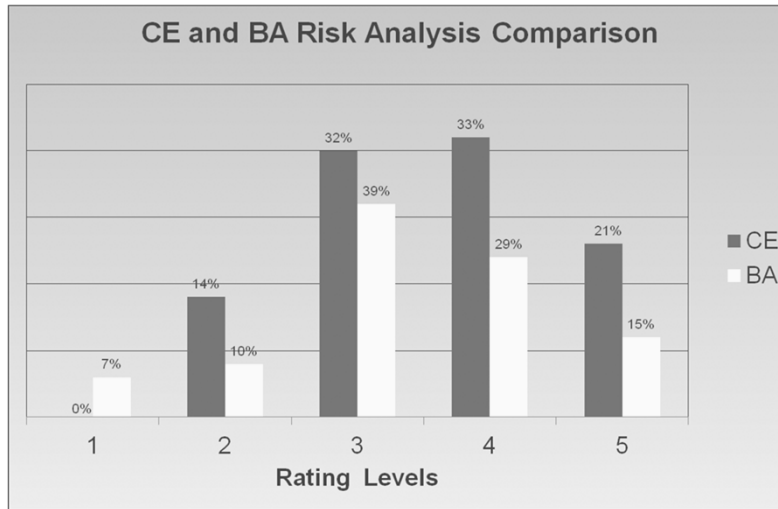
CEs: Privacy, Security and Breach Notification Rules

Rankings of the covered entities audited (103)						
Breach Rule	5	4	3	2	1	N/A
Timeliness of Notification	11%	9%	2%	6%	65%	7%
Content of Notification	7%	37%	23%	14%	14%	5%
Privacy Rule						
Provision of the NPP	15%	6%	4%	15%	57%	
NPP Content	15%	11%	39%	33%	2%	
Access right	11	54	27	10	1	
Security Rule						
Risk Analysis	13	23	19	8	0	
Risk Management	17	29	13	3	1	

BAs: Security and Breach Notification Rules

Rankings of the business associate audited (41)						
Breach Rule	5	4	3	2	1	N/A
Notification to CE	0%	7%	10%	5%	0%	78%
Security Rule						
Risk Analysis	15%	29%	39%	10%	7%	0%
Risk Management	17%	51%	20%	12%	0%	0%

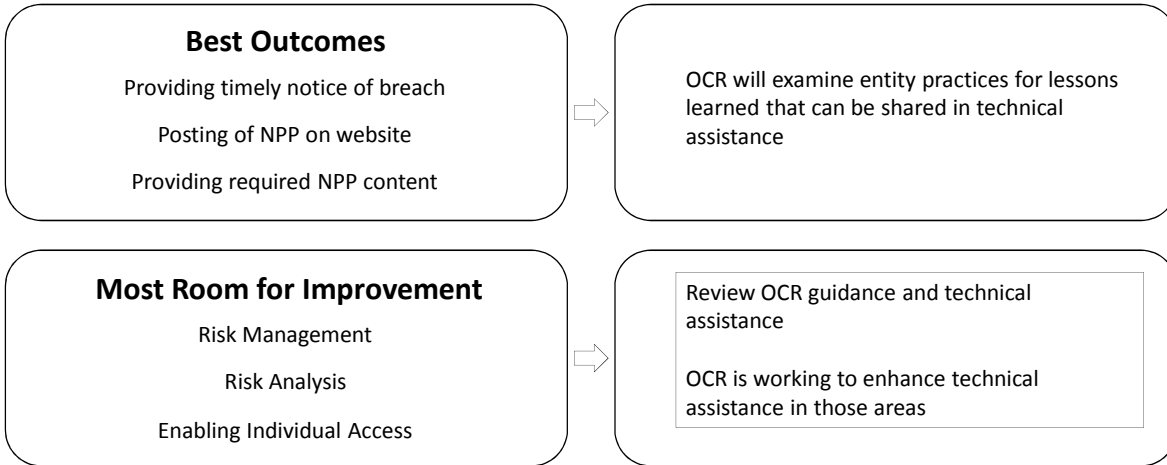
CE and BA Risk Analysis Comparison



CE and BA Risk Management Comparison



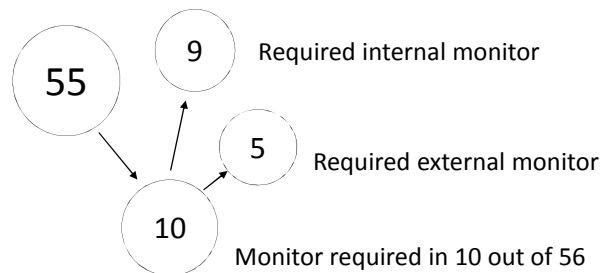
Industry Take-Away



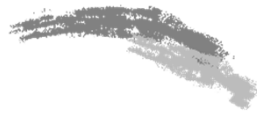
Enforcement Highlights

60 OCR enforcement actions
\$100 Million
 In settlements & CMPs
 13 settlements in 2016
 10 settlements in 2017
 6 settlement in 2018
 41 of 60
 enforcement actions
 arose from breach reports to
 HHS

4 Civil Money
 Penalty Actions
\$3,021,950
 Average settlement amount



Vendor Management Risks

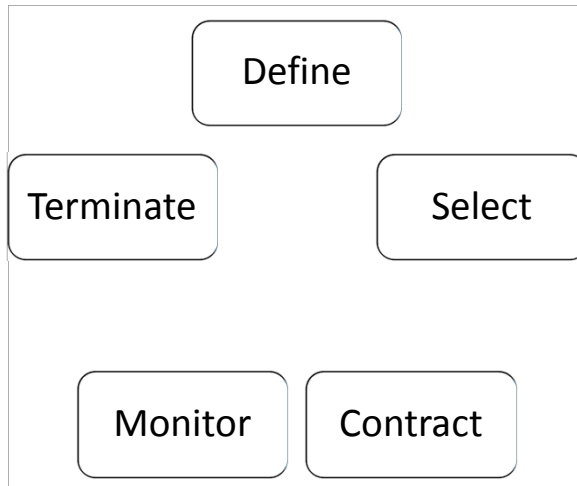


Healthcare Vendors in the News



Vendor Security Must Improve

- Requirements definition
- Pre-Contract due diligence
- Contract security specifications
- Performance monitoring
- Breach Notification
- Contract termination
- Documentation

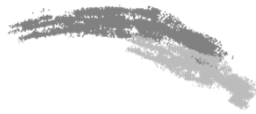


Breach Notification

- Contract language regarding
 - Security incident notification
 - Breach notification
- Timeliness of notifications
- Assistance in investigation/risk assessment
- Indemnification for certain costs
- Notifications to public



Compliance and Privacy Key Considerations Incident Response



Understanding who is in charge, the hierarchy.

- Who is in charge?
 - Who are the key stakeholders?
 - What are their priorities?
 - When are they needed?
 - How do you communicate?
 - When or if do you engage legal?

Specifically, Who To Involve

- Core team members
 - CIO
 - Multiple specialist across IT and IS
 - Compliance Leadership
 - CCO
 - CPO
 - CISO
 - General Counsel
 - Designated member of the senior leadership team
 - Business Unit Leaders
 - **Clinical Leadership**



Specifically, Who To Involve

- Key stakeholders representing other functions
 - Media relations
 - Patient relations
 - Procurement
 - Human Resources
 - Impacted business owners
 - Other senior leaders of your organization
 - CEO, CFO, CNO, CMO, & CMIO
 - Senior leaders of a parent organization



Specifically, Who To Involve

- Key outside stakeholders who may need to be involved
 - Cybersecurity insurance company
 - External counsel
 - Key vendors
 - Forensics firms
 - Support for response and recovery
 - Law enforcement
 - Local
 - Federal
 - Impacted business partners such as affiliated healthcare providers



Developing a Successful IRP

Develop **repeatable**, **efficient**, and **effective** incident response processes

Use these to **identify**, **analyze**, and **correct** hazards to prevent future occurrences

Four primary work components will help this initiative:

- Initiate and Organize: Establish Incident Response Project Governance
- Measure: Conduct Incident Response Workflow Analysis
- Standardize & Align: Develop Incident Response Program and Processes
- Perform & Inform: Post-Incident Activity



What is Often Missing From IRPs

- Executive Buy-in for planning and execution of IRP
- Governance Council Involvement in Planning & execution of IRP
- Breach notification and compliance
- Thorough communication plans (internal and external)
- Involvement beyond IT and IS departments
- Regular Exercises and updates
- Up-to-date phone trees



Notification to Covered Entities & Business Partners

- In addition to regulatory obligations to notify there may also be other obligations
 - Contractual obligations
 - Are you a BA to another covered entity?
 - Does the organization have contracts that require notification regarding a data incident or breach



Plenty of Ways to Get Ahead During the Attack

- Anticipate having to defend against legal consequences
 - Engage your GC early, especially if litigation is anticipation
 - Determine if Privilege is needed as soon as possible
 - Assign a scribe – who discovered what, when, & how
- Do not rush to reimage – it destroys evidence that can be used to support your conclusions
- Start documenting for the after action report now



Thank You!

Questions?

Marti Arvin
VP of Audit Strategy
marti.arvin@cynergistek.com
512.450.8550 x7051

