Your Business Associates and Other Issues: What You Don't Know Can Hurt You!

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

CYNERGISTEK

Meeting Agenda

✓ **Review Proposal Objectives, Process, Outputs, and Timeline.**

1. Vendor Management
2. OCR Desk Audit Results
3. Enforcement Trends
4. Questions

Privacy, Security, & Compliance Challenges:
Vendor Management

Healthcare Vendors in the News

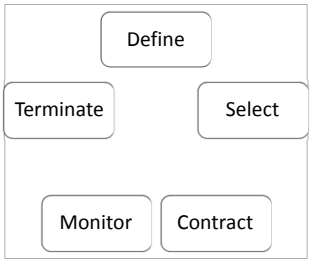
NUANCE

eClinicalWorks

Allscripts

Vendor Security Must Improve

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



Defining Requirements

- Examine scope of effort
- Determine what level of Minimum Necessary
- Identify security requirements
- Develop SLAs for Privacy and Security
- Incorporate into RFI, RFP and/or SOW
- Classify vendor
- Not all vendors create the same risk

Due Diligence: Pre-Contract

- Tailor requests to scope of contract
- Security standard followed
- Include privacy and security questionnaire
- Request documentation
- Review third-party assessments
- Proof of training
- Conduct site visit
- Privacy and security incident history

CYNERGISTEK 15

Contract Security Specifications

- Define expectations, material changes, subcontractors
- Minimum Necessary
- Transmission, storage & processing
- Incident response
- Audit/monitoring
- Reporting requirements
- Contingency operations

CYNERGISTEK 6

Maintenance

- For contracts lasting more than six months
- Periodic audits of key processes
- Testing of contingency plans/operations
- Renewal of third-party assessments

CYNERGISTEK 7

Breach Notification

- Timeliness of notifications
- Assistance in investigation/risk assessment
- Indemnification for certain costs
- Notifications to public

Contract Termination

- Termination for cause vs. end of contract
- Disposition of data if in receipt
- User/system access
- Reminder of Minimum Necessary
- Other continued responsibilities

Assessing for Compromise: Business Associate?

- Hospital vendor's pager network dispatches lab, imaging and respiratory services. Messages contain PHI. No business associate agreement in place.
  - PHI identifiable and sensitive
  - Stored on vendor's IT system
  - PHI acquired by vendor and workforce
  - BA agreement now in place
- Has PHI been "compromised?"

OCR Desk Audit Results

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 were significant threats to the privacy and security of PHI are revealed through the audit.

OCR Compliance Rating Scale

A ↕ F

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.

CYNERGISTEK 16

CEs: Privacy, Security and Breach Notification Rules

Rating at each end of the rankings for all entities (103)		
Breach Rule	5 Rating	1 Rating
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

CYNERGISTEK 17

CEs: Privacy, Security and Breach Notification Rules

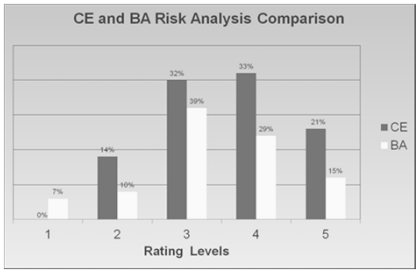
Rankings of the covered entities audited (103)						
Breach Rule	5	4	3	2	1	N/A
Timeliness of Notification	11%	9%	2%	6%	65%	7%
Content of Notification	7%	37%	23%	14%	14%	5%
Privacy Rule						
Provision of the NPP	15%	6%	4%	15%	57%	
NPP Content	15%	11%	39%	33%	2%	
Access right	11	54	27	10	1	
Security Rule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

CYNERGISTEK 18

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

Best Outcomes

Providing timely notice of breach

Posting of NPP on website

Providing required NPP content

OCR will examine entity practices for lessons learned that can be shared in technical assistance

Most Room for Improvement

Risk Management

Risk Analysis

Enabling Individual Access

Review OCR guidance and technical assistance

OCR is working to enhance technical assistance in those areas

CYNERGISTEK

22

Some Good News

- First the good news
  - The new OCR Director, Roger Severino, is quoted as saying, "No" to the question will there be a, "Phase three audit program" at the 2018 HIMSS conference in early March
  - He also stated that OCR was reviewing the regulations to see if they could reduce "undue burden" on the industry

Quoted from HealthcareInfoSecurity article March 6, 2018, available at https://www.healthcareinfosecurity.com/no-slowdown-for-hipaa-enforcement-but-audits-ending-a-10701

CYNERGISTEK

23

Now the Bad News

- Now the bad news
  - At the same HIMSS meeting, Director Severino was also quoted as saying, "We're looking for the big, juicy egregious cases" for enforcement and;
  - There is, "No slowdown in our enforcement efforts" and the agency will continue with the same "enforcement mindset."
  - Later in March 2018 at the 27th National HIPAA Summit, Director Severino revised the statement about no more audits made at the 2018 HIMSS meeting to say that there were not audits planned in the immediate future.
    - The requirement under HITECH for OCR to perform audits does not grant him the authority to discontinue the audits.

Quoted from HealthcareInfoSecurity article March 6, 2018, available at https://www.healthcareinfosecurity.com/no-slowdown-for-hipaa-enforcement-but-audits-ending-a-10701

CYNERGISTEK

24

Ransomware: Business Associate

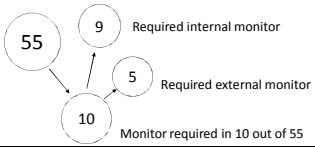
- Large ambulatory network infected with ransomware
  - Ransomware attempted to encrypt shared drives hosted on EHR hosting provider's servers - but quick detection allowed the link to be severed.
  - Virtual server was rebuilt and back online in approximately an hour.
  - The ambulatory network remained offline for over a week while the on-site networks and systems were rebuilt.

Enforcement Trends

Enforcement Highlights

55 OCR settlements
$79 Million
In settlements & CMPs
13 settlements in 2016
10 settlements in 2017
2 settlement in 2018
40 of 58
enforcement actions arose from breach reports to HHS

3 Civil Money Penalty Actions
$1,299,004
Average settlement amount



How May Cases Does OCR Handle?

Breaches Reported September 2009 through December 31, 2017

- >2,100 reports of breach of PHI affecting 500 or more individuals
- >305,000 reports of breaches affecting fewer than 500 individuals
- >200 million individuals affected by a breach involving their PHI

Investigations and Closures

- >171,000 complaints received since 2003
  - 66% are closed after intake & review
- Compliance review initiated into each breach affecting >500 individuals
- >25,600 cases/compliance reviews resolved with corrective action or technical assistance

Issues Raised in OCR Enforcement

- Most resolution agreements cite to Security Rule
  - Enterprise wide risk analysis is foundation
  - Managing/control of devices & media (& encryption)
- Assessment of organization when performing hybrid covered entity analysis
- Failure to have BA agreements with contractors, vendors, or corporate parent
- Using PHI for marketing without obtaining authorization
- Allowing media access to treatment areas without obtaining patient authorization
- Failure to perform timely breach notification

OCR Guidance Year in Review

- Themes behind guidance issued in 2016-18
  - How HIPAA Privacy and Security Rule apply to areas involving health IT
    - HIPAA and cloud computing
    - Ransomware and malware incidents
  - Patient access to their PHI, sharing PHI with third parties and fees that can be charged
  - Disclosures of PHI through health IT and health information exchange permitted for treatment and health care operations

Serious & Imminent Threat to Health

- OCR guidance modifies permitted disclosures to prevent serious and imminent threat to health & safety
- Example: Doctor whose patient has overdosed on opioids believes patient poses serious & imminent threat to his or her health through continued opioid abuse upon discharge; informs friends & family
- Prior guidance that it applies in those rare circumstances that threat is extremely time sensitive and urgent conditions to clear & present danger
- Can this be applied to other types of scenarios?
- "Traditional" Privacy Rule required demonstrable, particularized, & imminent threat

Thank You!

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