1

Cyber Security and Health Care Privacy

HCCA HEALTHCARE ENFORCEMENT COMPLIANCE CONFERENCE,
WASHINGTON, D.C., NOVEMBER 3, 2019

Marti Arvin — CynergisTek
Joseph Dickinson — Smith Anderson
David Kessler — Verizon
Roy Wyman, Moderator — Nelson Mullins

1

2

Cyber Security and Health Care Privacy

The Current Cyber Security and Privacy Legal Landscape and Enforcement Actions

2

3

Emerging Technologies:
Cyber Security and Privacy Risks
for Healthcare-related Entities

3

4

Addressing Risks from Supply Chain and
Third-party Vendors to Reduce Enforcement Risks

4

5

Appendix: Additional Materials

5

6

Privacy, Security, & Compliance Challenges: Vendor Management

6

7

Healthcare Vendors in the News

NUANCE

eClinicalWorks

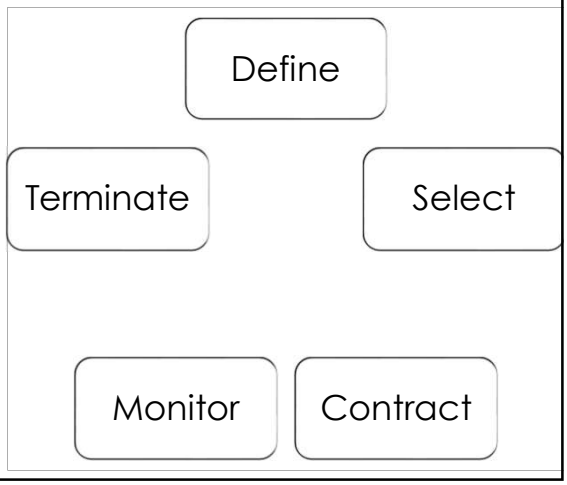
Allscripts

7

8

Vendor Security Must Improve

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



8

9

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

9

10

Due Diligence: Pre-Contract

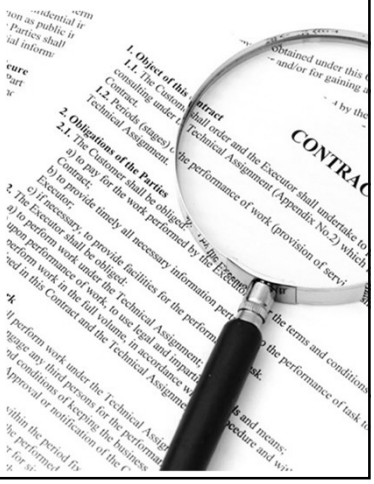
- Tailor requests to scope of contract
- Security standard followed
- Include privacy and security questionnaire
- Request documentation
- Review third-party assessments
- Proof of training
- Conduct site visit
- Privacy and security incident history

10

11

Contract Security Specifications

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



11

12

Maintenance

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

12

13

Breach Notification

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

13

14

Contract Termination

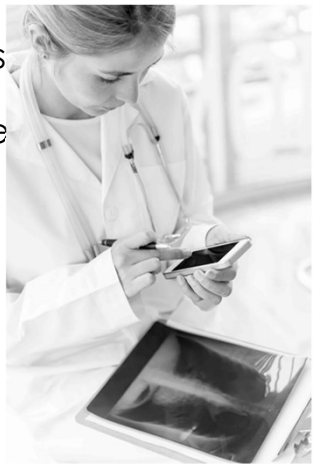
- Termination for cause vs. end of contract
- Disposition of data if in receipt
- User/system access
- Reminder of Minimum Necessary
- Other continued responsibilities

14

15

Assessing for Compromise: Business Associate?

- Hospital vendor's pager network dispatches imaging and respiratory services. Messages contain PHI. No business associate agreeme 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?"



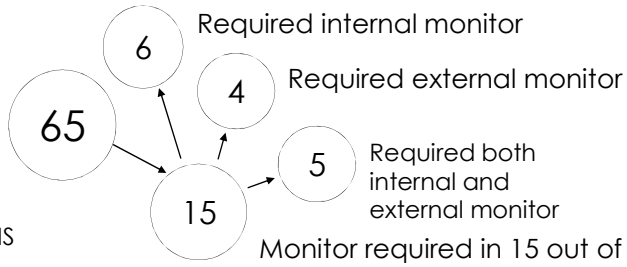
15

16

Enforcement Highlights

63 OCR Settlements
$107 Million
In settlements & CMPs
13 settlements or CMPs in 2016
9 settlements or CMPs in 2017
11 settlements or CMPs in 2018
2 settlements or CMPs in 2019
42 of 67
enforcement actions
arose from breach reports to HHS

4 Civil Money
Penalty Actions
$12,087,800 Total CMPs



Monitor required in 15 out of 63

16

17

Recent Cases of Interest

Touchstone Medical Imaging, LLC

- Records exposed almost 308K
- Settlement amount $3,000,000
- OCR got an email informing it of the data compromise
- FBI alert TMI the same day
- 2 year RA/CAP

17

18

Recent Cases of Interest

Touchstone Medical Imaging, LLC

- Findings
  - Impermissibly exposed the records of almost 308 K individuals
  - Failed to implement technical P & Ps to limit access to FTP servers
  - Failure to have timely BAA (issue identified 5/14, BAA entered 6/16)
  - Failure to have any BAA, as of RA/CAP TMI still had not entered BAA
  - No risk analysis until 4/14
  - Failure to timely respond to known security incident, 5/9/14 to 9/26/14
  - Failure to timely notify individuals and media, breach discovered 5/9/14 notification occurred 10/3 and 10/4 respectively

18

HCCA Enforcement Compliance Conference

Cyber Security and Health Care Privacy

November 3, 2019

19

New technology? Vendor? Cloud?

- Update your Risk Analysis
- Update relevant policies and procedures
- Update your data map
- Understand data flow and how and where data is processed
- Understand access points
- Servers/SaaS/IaaS/PaaS- configurations
- HIPAA requires more than just an annual review
- If there is a breach OCR should and will look closely at this

20

20

Updates To Risk Analysis

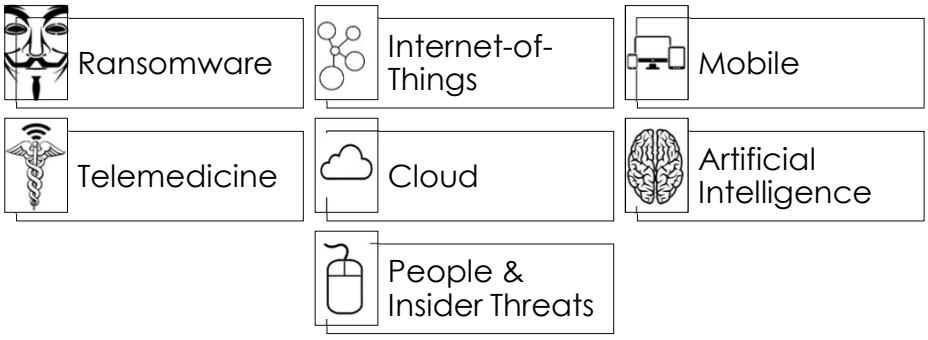
- New or Material Change in Uses/Disclosures of PHI
- Data Maps/Asset Inventories
  - Accurate?
  - Reflect real world?
  - Don't rely on terms of contracts

Risk Analysis?

- Existing?
  - If not, why not?
- Review before agreeing on contract terms
- Is an update needed after execution?
- M&A inherited risk?
- Is client aware of the risks?
  - Existing incidents? Breaches? Bad policies?

23

Emerging technologies: Cybersecurity and privacy risks for healthcare-related entities



23

24

Current & Future Regulatory Landscape

24