ATTAC CONSULTING GROUP
healthcare solutions ▲ business results

Data Security Maturity

Ensuring your Plan Sponsor's FDRs employ robust data security through effective delegate oversight.

1

ATTAC CONSULTING GROUP

Erin Miskell, J.D., Consultant
ATTAC Consulting Group, LLC

- University of South Carolina School of Law, 2006
- Private practice: family and criminal law
- Bravo Health-2007, A&G, Cust. Service, Project Management, Compliance.
- XLHealth-2011, Compliance and Audit
- UHC 2012-Distribution Compliance, Delegated Entity Oversight
- ATTAC Consulting Group 2018, primarily in Compliance Solutions

2

2

2.65 Million Atrium Health Patients Impacted by Business Associate Data Breach Vendor/Delegate-Hacking/IT Incident

- AccuDoc Solutions Inc., a provider of healthcare billing services, has experienced a major data breach in which the protected health information of 2,650,000 patients of Atrium Health was exposed.
- AccuDoc Solutions reports that the breach was due to a security vulnerability at a third-party vendor. System and info were accessed but no data downloaded.

https://www.hipaajournal.com/2-65-million-atrium-health-patients-impacted-by-business-associate-data-breach/

https://www.modernhealthcare.com/article/20181128/NEWS/181129940/2-65-million-atrium-health-patients-data-potentially-exposed

3

3

9,497 Consumers' Data Compromised by Laptop Theft Employee-Unauthorized Access/ Disclosure

- In March 2016, North Memorial Health Care of Minnesota was hit with a $1.55 million settlement with HHS stemming from the 2011 theft of an unencrypted laptop from a staff member's vehicle.
  - Critical HIPAA – related errors:
    - Failure to have a compliant business associate agreement in place
    - Failure to employ a thorough risk analysis that addresses enterprise-wide IT infrastructure.

https://www.healthcareitnews.com/news/ocr-settles-two-hipaa-breach-suits-totaling-55-million-north-memorial-health-care-Feinstein

https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/north-memorial-health-care/index.html

4

4

California Dept. of Developmental Services Notifies 582,000 Patients of Potential PHI Compromise; Physical Premises – Equipment Theft and Physical Access Violation

- Thieves broke into the DDS legal and audits offices in Sacramento, CA, stole 12 (encrypted) computers. During the time they were in the office, they potentially had access to member and employee data.
- The security breach is the largest to be reported to OCR in 2018.

https://www.hipaajournal.com/california-dept-of-developmental-services-582000-patients-phi/

https://www.sacbee.com/news/politics-government/the-state-worker/article208185014.html

5

5

Top 5 HIPAA Breaches of 2018- source

Rank	Name of Covered Entity	Covered Entity Type	Individuals Affected	Type of Breach
1	AccuDoc Solutions Inc.	Business Associate	2,652,537	Hacking/IT Incident
2	UnityPoint Health	Business Associate	1,421,107	Hacking/IT Incident
3	Employees Retirement system of Texas	Health Plan	1,248,263	Unauthorized Access / Disclosure
4	CA Department of Developmental Services	Health Plan	582,174	Theft
5	MSK Group	Healthcare Provider	566,236	Hacking/IT Incident

https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2018/

6

6

Why Is HIPAA Compliance Important?

HIPAA compliance guidelines are incredibly essential. Failure to comply can put patients' health information at risk. Breaches affect your company's reputation, and you could be subject to disciplinary action and strict violation fines and penalties.

7

7

40 – Sponsor Accountability for Oversight of FDRs

- The sponsor maintains the ultimate responsibility for fulfilling the terms and conditions of its contract with CMS, and for meeting the Medicare program requirements.
- The sponsor's compliance officer, working with the sponsor's compliance committee, must develop procedures to promote and ensure that all FDRs are in compliance with all applicable laws, rules and regulations with respect to Medicare Parts C and D delegated responsibilities.
- Sponsors must be able to demonstrate that their method of monitoring is effective.

8

8

Delegates and HIPAA Security

- HIPAA guidelines protect patients' health information, requiring covered entities to ensure it is stored and transmitted securely, and disclosed only to appropriate recipients.
- The safeguards of the HIPAA Security Rule are broken down into three main sections. These include technical, physical, and administrative safeguards.
  - Technical- Systems
  - Administrative - Policies
  - Physical – Access Restrictions

9

9

Data Security Examples

- Laptops-
  - Are they locked down physically so they can't be stolen?
  - Are they able to be scrubbed if they're lost or stolen?
- Data Centers-
  - Are there specific permissions required for who may enter?
  - Is there related monitoring of access to the physical spaces?
- Medical Records-
  - Are there limitations and permissions employed for who may view records?
  - Is there monitoring of who accesses medical records, and whether they're authorized to do so?

10

10

ATTAC CONSULTING GROUP

Effective Oversight of FDR Data Security

- Good contract discipline
  - BAA- https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html
  - Breach reporting requirements
- Ongoing monitoring and auditing of data security protocols
- Education of internal and external stakeholders
- Effective disciplinary methods including Corrective Action Plans
- Specific methods- pre-delegation audit, annual attestation or security checklist, risk-based audit, random audit

11

11

ATTAC CONSULTING GROUP

What is the HIPAA Privacy Rule?

- The HIPAA Privacy Rule implements national standards designed to protect medical records and other protected health information (PHI).
- Health plans of all kinds must be HIPAA compliant, as must providers, healthcare data centers and many other types of healthcare service organizations.
  - **Covered entities** are defined in the **HIPAA** rules as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards.
- Under the Privacy Rule, all covered entities must employ safeguards to protect patient privacy and disclosure of PHI, whether electronic or hard copy.

https://privacyruleandresearch.nih.gov/pr_06.asp

12

12

What Is The HIPAA Security Rule

- All e-PHI created, received, maintained or transmitted by an organization is subject to the Security Rule.
- The Security Rule requires entities to evaluate risks and vulnerabilities in their environments and to implement reasonable and appropriate security measures to protect against reasonably anticipated threats or hazards to the security or integrity of e-PHI.
- Risk analysis is the first step in that process.

https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html?language=es

13

13

Scope of the Analysis

The scope of risk analysis that the Security Rule encompasses includes:

- The potential risks and vulnerabilities to the confidentiality, availability and integrity of all e-PHI that an organization creates, receives, maintains, or transmits. (45 C.F.R. § 164.306(a).)
- This includes e-PHI in all forms of electronic media.
- Electronic media includes a single workstation as well as complex networks connected between multiple locations.

Your organization's risk analysis should take into account all of its e-PHI, regardless of the particular electronic medium in which it is created, received, maintained or transmitted or the source or location of its e-PHI.

https://www.ncmedsoc.org/wp-content/uploads/2016/04/Security-Risk-Analysis-for-HIPAA-Compliance.pdf

14

14

Offshore Delegate CMS Requirements

CMS outlined the items to which Sponsors must attest, as CMS seeks to ensure Plans employ safeguards to protect beneficiary information in the offshore subcontract. These elements are:

- Offshore subcontracting arrangement has polices and procedures in place to ensure that PHI and other personal information remains secure.
- Offshore subcontracting arrangement prohibits subcontractor's access to data not associated with the sponsor's contracts.
- Offshore subcontracting arrangement has policies and procedures in place that allow for immediate termination of the subcontract upon discovery of a significant security breach.
- Offshore Subcontracting arrangement includes all required Medicare Part C and D language.

15

15

Offshore Delegate CMS Requirements

Additionally, CMS included the language Sponsors must agree to in the attestation of audit requirements to ensure protection of PHI. These are:

- Organization will conduct an annual audit of the offshore subcontractor.
- Audit results will be used by the Organization to evaluate the continuation of its relationship with the offshore subcontractor.
- Organization agrees to share offshore subcontractor's audit results with CMS, upon request.

"I'll be in charge of delegating all the blame."

16

16

HIPAA Compliance for Delegates- The Basic Checklist

- Have you identified all delegated entities?
- Do you have a Business Associate Agreement (Business Associate Contract) in place with each delegated entity?
- Have you audited your delegated entities to make sure they are compliant with HIPAA rules?

- Do you have monitoring and auditing reports to prove your due diligence regarding your delegated entities, as well as CAP actions and results?
- Do you have systems in place to allow you to track and manage investigations of any incidents that impact the security of PHI?
  - Can you demonstrate that you have investigated each incident?
  - Can you provide reporting of all breaches and incidents, whether they are minor or meaningful?

17

17

HIPAA Compliance for Delegates- The Basic Checklist

- Have you created a solid compliance structure for delegation oversight, including good contracting practices, thorough pre-delegation auditing, ongoing monitoring and auditing plans, and delegation oversight committee?
  - Not just for regulatory and operational activity, but also good HIPAA security practices
- Is there a system in place so staff members may anonymously report an incident if the need arises?

18

18

Sum Up

Plan Sponsors Must:

- Fully implement an effective compliance program
- Understand and implement HIPAA Security requirements.
- Implement a thorough and effective delegated entity oversight program including:
  - Prevention- good contract practices, training, education, risk assessments
  - Detection- monitoring and auditing, investigation of suspected offenses
  - Correction- corrective actions, termination
- Employ effective breach reporting processes.

19

19

Questions?

20

20