Scalable Vendor Due Diligence- How to Effectively Evaluate Business Associates

Mark J. Fox CHC,CHPC,CHRC
Privacy and Research
Compliance Officer

AMERICAN COLLEGE of CARDIOLOGY

The General Provision

The Privacy Rule requires that a Covered Entity obtain satisfactory assurances from a Business Associate that Business Associate will appropriately safeguard the Protected Health information it receives or creates on behalf of a Covered Entity. The satisfactory assurances must be in writing, whether in the form of a contract or other agreement between the Covered Entity and the Business Associate.

Business Associate Agreement

- Develop a template Business Associate Agreement.
- Require indemnification for breaches of the Business Associate Agreement.
- Consider prohibition of offshoring by the Business Associate.
- Develop best alternative to negotiated agreement for all provisions of your Business Associate Agreement.

Cyber Liability Insurance

- Require that all Business Associates maintain Cyber Liability Insurance .
- Establish minimum coverage requirements.
- Insert requirement to carry Cyber Liability Insurance in underlying agreement or Business Associate Agreement.
- Require that all Business Associates submit a Certificate of Insurance.

AMERICAN COLLEGE of CARDIOLOGY

Security Questionnaires

- Develop a standard security questionnaire for your Business Associates.
- Require business lines to develop Statements of Work for your Business Associates before evaluating responses to the security questionnaire.
- Determine minimum requirements for passing a due diligence assessment.

Security Questionnaires

- Use a risk based approach to determining if a Business Associate has adequate controls in place.
- Evaluate the level of dependency your organization has on each Business Associate and consider contingencies.

Risk Assessments

- Will your Business Associate share the results of their annual risk assessment?
- Consider requiring a management letter from your Business Associates confirming completion of a risk assessment and including high level findings of the risk assessment.

Third Party Evaluation

- Do you have adequate funding to outsource due diligence to a third party vendor?
- Consider asking your Business Associates if they have completed a independent control assessment?
- Ask Business Associates to provide a management letter from the third party assessor confirming completion and sharing high level results.

Breach Response

- Ensure that your Business Associates know who to notify when an impermissible disclosure or Breach of Unsecured Protected Health Information occurs.
- Obtain contact information of the Privacy Officer and Information Security Officer at each Business Associate.

Breach Response

- Ensure that roles and responsibilities for breach response are articulated in the Business Associate Agreement.
- Ensure that you periodically ask for updated contact information for the Privacy Officer and Information Security Officer at each Business Associate.
- Evaluate indemnification provisions of the Business Associate Agreement.

Remediation

- Following a breach evaluate each Business Associate involved in the breach and require corrective action plans when warranted.
- Consider targeted reevaluation of Business Associate relationships including resubmission of a security questionnaire.
- Also consider if there has been a breach of the underlying agreement or Business Associate agreement and steps of remediation.

Ongoing Evaluation

- Determine frequency of reevaluation of existing Business Associate relationships.
- Be realistic in the expectations set for reevaluation.
- Consider a risk based approach to reevaluation based on the scope of each Business Associate relationship.

Questions and Discussion

AMERICAN COLLEGE of CARDIOLOGY

References

- Business Associates. (n.d.). Retrieved February 17, 2020, from https//www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html

AMERICAN COLLEGE of CARDIOLOGY

AMERICAN COLLEGE *of* CARDIOLOGY