

Collections: Business Associate Assessment - HIPAA-HITECH-Omnibus Privacy and Security Summary Report

Assessment Risk: Medium (22)

Documented Evidence: 61.1%


 **Assessment Details**

Organization: Collections

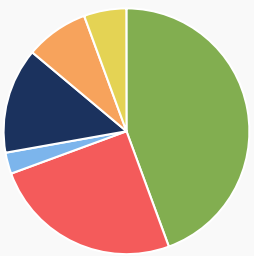
Profile Risk Tier: Medium

Profile Risk Notes:

Assign Date:	February 17, 2017	Assignees:	Bill Reiher
Finish Date:	February 17, 2017	Assigned By:	Ken Reiher
Time to complete:	20 minutes	Categories:	HIPAA / HITECH Security, HIPAA Privacy

 **Question Summary:**

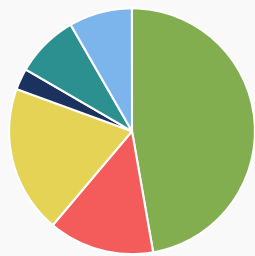
Documented Evidence:



- 44.4% Yes (16)
- 25.0% No (9)
- 2.8% Not Assigned (1)
- 13.9% Not applicable (5)
- 8.3% To be determined (3)
- 5.6% Partial (2)

61.1% Documented Evidence

Risk:



- 47.2% Low (1) (17)
- 13.9% High (100) (5)
- 19.4% Medium (25) (7)
- 2.8% Not Required (1)
- 8.3% Low-Medium (5) (3)
- 8.3% Not applicable (0) (3)

88% Assigned Risk

Answers with Notes:
36% - (13/36)

Answers with Attachments:
19% - (7/36)

Rule Risk Breakdown:

Information System Activity Review (Required) High (100)

- Create and implement a formal policy and procedure for information system activity review.

Workforce security High (100)

- Create and implement a formal process for assigning and terminating workforce access to PHI and ePHI.

Termination procedures (Addressable) High (100)

Risk Analysis (Required) Medium (50)

- Implement periodic intrusion vulnerability, penetration testing. - Due on: 3/31/2017
- Provide evidence documentation

Implementation Specifications: Business Associate Contracts Medium (34)

Risk Management (Required) Medium (25)

- Provide the name of the software used and proof of its existence.

Business associate contracts (Required) Medium (25)

Policies and Procedures. Medium (25)

Access of Individuals to Protected Health Information Medium (25)

Security incident procedures. Medium (13)

Audit controls. Medium (13)

Contingency plan. Low (5)

Facility access controls. Low (5)

Policies and procedures and documentation requirements. Low (5)

Security Management Process Low (1)

Sanction Policy (Required) Low (1)

Information access management. Low (1)

Security awareness and training. Low (1)

Evaluation. Low (1)

Workstation use. Low (1)

Device and media controls. Low (1)

Data backup and storage (Addressable) Low (1)

Access control. Low (1)

Encryption and decryption (Addressable) Low (1)

Encryption (Addressable) Low (1)

Implementation Specifications: Other Requirements for Contracts and Other Arrangements Low (1)

Assigned security responsibility. TBD