ComplyAssistant

Assessment: Completion Summary

Assessment Details: Business Associate Assessment - HIPAA-HITECH-Omnibus Privacy and Security

Description:	As Ken Reiher mentioned in his initial email, this is General Hospital's vendor privacy and security assessment, prepared by ComplyAssistant. Please answer each question as fully as you can to assist SP in satisfying its due diligence regarding vendor privacy and security practices. If you have any issues or concerns with the tool, please contact: Bruce Pugh IT Security and HIPAA Consultant, ComplyAssistant bruce.pugh@complyassistant.com 800-609-3414 Ext. 709.
Organization:	Collections
Profile Risk Tier:	Medium
Profile Risk Notes:	

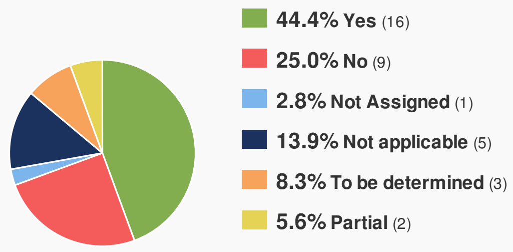
Assign Date:	February 17, 2017	**Assignees:**	Bill Reiher
Finish Date:	February 17, 2017	**Assigned By:**	Ken Reiher
Priority:	High		
Categories:	HIPAA / HITECH Security, HIPAA Privacy		
Status:	No Tasks		
Frequency:	None		

General Comments

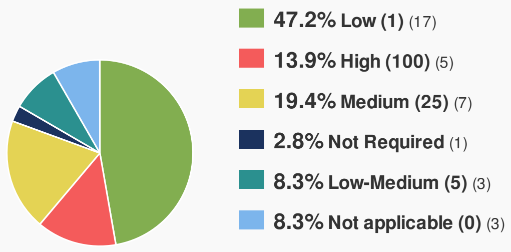
Gerry Blass
Please review
Aug 26, 2017 at 10:52AM

Review:

Documented Evidence:



Risk:

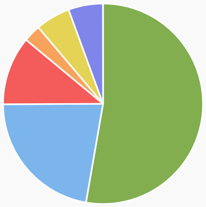


61.1% Documented Evidence

Average Risk: Medium (22)

Summary: Completed on 2/17/2017 - **100% complete (36/36)**

Answers:



- 🟩 **52.8% Yes** (19)
- 🟦 **22.2% Free Answer** (8)
- 🟥 **11.1% No** (4)
- 🟧 **2.8% Don't Know** (1)
- 🟨 **5.6% Partial** (2)
- 🟪 **5.6% Not Applicable** (2)

Answered By:

- 🟦 **100.0% Ken Reiher** (36)

Answers with Notes:

36% - (13/36)

Answers with Attachments:

19% - (7/36)

Rule Risk Breakdown:

Information System Activity Review (Required) • Create and implement a formal policy and procedure for information system activity review.	High (100)
Workforce security • Create and implement a formal process for assigning and terminating workforce access to PHI and ePHI.	High (100)
Termination procedures (Addressable)	High (100)
Risk Analysis (Required) • Implement periodic intrusion vulnerability, penetration testing. - Due on: 3/31/2017 • Provide evidence documentation	Medium (50)
Implementation Specifications: Business Associate Contracts	Medium (34)
Risk Management (Required) • Provide the name of the software used and proof of its existence.	Medium (25)
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

1) Does your organization have a written Security Management Program in place for information security? (Please note that when answering every question in this assessment that you must also add notes to explain your answer,and attach evidence documents such as policies and procedures, and operational compliance in relation to the question. You do not need to attach the same document to more than 1 question if it applies to more than 1.)

Answer: Yes

Notes: See attached documentation

Attachments:

Security_management_process.pdf (2.95 KB) 2/17/2017 by Ken Reiher

Answered by Ken Reiher on Feb 17, 2017 at 8:59AM and updated on Feb 17, 2017 at 9:22AM

Risk: ○ Not applicable ● Low (1) ○ Low-Medium (5) ○ Medium (25) ○ Medium-High (50) ○ High (100)

Documented Evidence: ● Yes ○ No ○ Partial ○ To be determined ○ Not applicable

Tasks:

Question Reference: If yes, please describe your overall security management program, as appropriate. If answering partial, please describe what aspects of a security management program have been implemented.

Business Associates are required to comply with the Security Rule at 164.308(a)(1) and implement a security management process with policies and procedures to prevent, detect, contain, and correct security violations.

HIPAA / HITECH Security

- Part 164 - Security and Privacy
  - 164 - Subpart C - Security Standards for the Protection of Electronic Protected Health Information
    - 164.308 - Administrative safeguards.
      - **164.308(a)(1)(i) - Security Management Process**

Description: Standard. Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations.

Things To Consider: OCR Audit Protocol.

Acquire IT Systems and Services. Required.
Security Management Process - Although the HIPAA Security Rule does not require purchasing any particular technology, additional hardware, software, or services may be needed to adequately protect information. Considerations for their selection should include the following:
-Applicability of the IT solutions to the intended environment;
-The sensitivity of the data;
-The organization's security policies, procedures, and standards; and
-Other requirements such as resources available for operation, maintenance, and training.

2) Does your organization routinely conduct and review HIPAA Risk Assessments/Analyses?

Answer: Yes

Notes: 2016 risk analysis attached

Attachments:

Risk_Analysis_2016.pdf (2.74 KB) 2/17/2017 by Ken Reiher

Answered by Ken Reiher on Feb 17, 2017 at 9:00AM and updated on Feb 17, 2017 at 9:22AM

Risk: ○ Not applicable ● Low (1) ○ Low-Medium (5) ○ Medium (25) ○ Medium-High (50) ○ High (100)

Documented Evidence: ● Yes ○ No ○ Partial ○ To be determined ○ Not applicable

Tasks:

Question Reference: If answering yes or partial, please provide the date on which your last risk analysis was performed/reviewed and explain the scope of the risk analysis. Please also identify any guidance used to perform the risk analysis (i.e., NIST or OCR guidance).

Business Associates are required by § 164.308(a)(1)(ii)(A) to perform a risk assessment on a routine and periodic basis which includes an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the business associate. Please see guidance which is available from OCR and NIST for conducting a Security Risk Assessment.

HIPAA / HITECH Security

- Part 164 - Security and Privacy
  - 164 - Subpart C - Security Standards for the Protection of Electronic Protected Health Information
    - 164.308 - Administrative safeguards.
      - 164.308(a)(1)(i) - Security Management Process
        - **164.308(a)(1)(ii)(A) - Risk Analysis (Required)**

Description: Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

Things To Consider: A thorough and accurate risk analysis would consider "all relevant losses" that would be expected if the security measures were not in place. "Relevant losses" would include losses caused by unauthorized uses and disclosures and E15loss of data integrity that would be expected to occur absent the security measures. Your organization's risk assessment process should address malicious software, such as computer viruses and "Trojan horses". You should also have a process to ensure that all electronic protected health information is appropriately identified and labeled (e.g., servers, workstations and all media - including backup tapes, CDs, diskettes, and other storage devices). If your organization decides not to implement an addressable specification, then do you have the appropriate management acknowledgement and documentation of that decision? You may want to consider having a third party periodically review your security procedures.