HIPAA Compliance Checklist

Healthcare Services, Inc. / 5 May 2023 / Shay Park

Complete

Score	97.87%	Flagged items	1	Actions	1

Institution	Healthcare Services, Inc.
Conducted on	05.05.2023 08:30 PST
Prepared by	Shay Park
Location	New Jersey, USA (40.07313198293444, -74.7243230220377)

Flagged items & Actions

1 flagged, 1 action

Flagged items

1 flagged, 1 action

Audit / Administrative Safeguards

164.308(a)(1)(ii)(D) Have you implemented procedures to regularly review records of IS activity such as audit logs, access reports, and security incident tracking? (R)

Non-Compliant

While there are procedures in place, these haven't been strictly implemented for the past two quarters. The most recent records review that is compliant was in Q1, while the Q2 and Q3 records reviews for FY 2022-2023 were conducted beyond schedule and have missing documentation. In this regard, our information security and privacy compliance officers are expected to supply due documentation and notices before the end of Q4.

FY22-23 Q2 Records Review - Timeline & Results.pdf

FY22-23 Q3 Records Review - Timeline & Results.pdf

To Do | Assignee SafetyCulture Staff | Priority Low | Due 11.05.2023 08:56 PST | Created by SafetyCulture Staff

Information security and privacy compliance officers to provide documentation and notices re: Q2 and Q3 records reviews.

Other actions

0 actions

Audit 1 flagged, 1 action, 97.87%

(R) = Required
(A) = Addressable

Administrative Safeguards

1 flagged, 1 action, 95.65%

164.308(a)(1)(i) Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations.

164.308(a)(1)(ii)(A) Has a Risk Analysis been completed IAW NIST Guidelines? (R)

Compliant

164.308(a)(1)(ii)(B) Has the Risk Management process been completed IAW NIST Guidelines? (R)

Compliant

164.308(a)(1)(ii)(C) Do you have formal sanctions against employees who fail to comply with security policies and procedures? (R)

Compliant

Please refer to the attached file to know more about the official formal sanctions.

Formal Sanctions - Violations on Security SOPs.pdf

164.308(a)(1)(ii)(D) Have you implemented procedures to regularly review records of IS activity such as audit logs, access reports, and security incident tracking? (R)

Non-Compliant

While there are procedures in place, these haven't been strictly implemented for the past two quarters. The most recent records review that is compliant was in Q1, while the Q2 and Q3 records reviews for FY 2022-2023 were conducted beyond schedule and have missing documentation. In this regard, our information security and privacy compliance officers are expected to supply due documentation and notices before the end of Q4.

FY22-23 Q2 Records Review - Timeline & Results.pdf

FY22-23 Q3 Records Review - Timeline & Results.pdf

To Do | Assignee SafetyCulture Staff | Priority Low | Due 11.05.2023 08:56 PST | Created by SafetyCulture Staff

Information security and privacy compliance officers to provide documentation and notices re: Q2 and Q3 records reviews.

164.308(a)(2) Assigned Security Responsibility: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.

Compliant

164.308(a)(3)(i) Workforce Security: Implement policies and procedures to ensure that all members of its workforce have appropriate access to EPHI, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information (EPHI).

164.308(a)(3)(ii)(A) Have you implemented procedures for the

Compliant

authorization and/or supervision of employees who work with EPHI or in locations where it might be accessed? (A)	
164.308(a)(3)(ii)(B) Have you implemented procedures to determine that the Access of an employee to EPHI is appropriate? (A)	Compliant
164.308(a)(3)(ii)(C) Have you implemented procedures for terminating access to EPHI when an employee leaves you organization or as required by paragraph (a)(3)(ii)(B) of this section? (A)	Compliant
164.308(a)(4)(i) Information Access Management: Implement policies and procedures for authorizing access to EPHI that are consistent with the applicable requirements of subpart E of this part.	
164.308(a)(4)(ii)(A) If you are a clearinghouse that is part of a larger organization, have you implemented policies and procedures to protect EPHI from the larger organization? (A)	Compliant
164.308(a)(4)(ii)(B) Have you implemented policies and procedures for granting access to EPHI, for example, through access to a workstation, transaction, program, or process? (A)	Compliant
164.308(a)(4)(ii)(C) Have you implemented policies and procedures that are based upon your access authorization policies, established, document, review, and modify a user's right of access to a workstation, transaction, program, or process? (A)	Compliant
164.308(a)(5)(i) Security Awareness and Training: Implement a security awareness and training program for all members of its workforce (including management).	
164.308(a)(5)(ii)(A) Do you provide periodic information security reminders? (A)	Compliant
164.308(a)(5)(ii)(B) Do you have policies and procedures for guarding against, detecting, and reporting malicious software? (A)	Compliant
164.308(a)(5)(ii)(C) Do you have procedures for monitoring login attempts and reporting discrepancies? (A)	Compliant
164.308(a)(5)(ii)(D) Do you have procedures for creating, changing, and safeguarding passwords? (A)	Compliant
164.308(a)(6)(i) Security Incident Procedures: Implement policies and procedures to address security incidents.	
164.308(a)(6)(ii) Do you have procedures to identify and respond to suspected or know security incidents; mitigate to the extent practicable, harmful effects of known security incidents; and document incidents and their outcomes? (R)	Compliant
164.308(a)(7)(i) Contingency Plan: Establish (and implement as needed) policies and procedures for	

responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain EPHI.

164.308(a)(7)(ii)(A) Have you established and implemented procedures to create and maintain retrievable exact copies of EPHI? (R)	Compliant
164.308(a)(7)(ii)(B) Have you established (and implemented as needed) procedures to restore any loss of EPHI data that is stored electronically? (R)	Compliant
164.308(a)(7)(ii)(C) Have you established (and implemented as needed) procedures to enable continuation of critical business processes and for protection of EPHI while operating in the emergency mode? (R)	Compliant
164.308(a)(7)(ii)(D) Have you implemented procedures for periodic testing and revision of contingency plans? (A)	Compliant
164.308(a)(7)(ii)(E) Have you assessed the relative criticality of specific applications and data in support of other contingency plan components? (A)	Compliant
164.308(a)(8) Have you established a plan for periodic technical and non technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of EPHI, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart? (R)	Compliant

164.308(b)(1) Business Associate Contracts and Other Arrangements: A covered entity, in accordance with Sec. 164.306, may permit a business associate to create, receive, maintain, or transmit EPHI on the covered entity's behalf only of the covered entity obtains satisfactory assurances, in accordance with Sec. 164.314(a) that the business associate appropriately safeguard the information.

164.308(b)(4) Have you established written contracts or other arrangements with your trading partners that documents satisfactory assurances required by paragraph (b)(1) of this section that meets the applicable requirements of Sec. 164.314 (a)? (R)	Compliant

Physical Safeguards

100%

164.310(a)(1) Facility Access Controls: Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

164.310(a)(2)(i) Have you established (and implemented as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency? (A)	Compliant

164.310(a)(2)(ii) Have you implemented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft? (A)	Compliant
164.310(a)(2)(iii) Have you implemented procedures to control and validate a person's access to facilities based on their role or function,	Compliant
including visitor control, and control of access to software programs for testing and revision? (A)	Compliant
164.310(a)(2)(iv) Have you implemented policies and procedures to document repairs and modifications to the physical components of a	Compliant
facility, which are related to security (for example, hardware, walls, doors, and locks)? (A)	Compliant
164.310(b) Have you implemented policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access EPHI? (R)	Compliant
164.310(c) Have you implemented physical safeguards for all workstations that access EPHI to restrict access to authorized users? (R)	Compliant

164.310(d)(1) Device and Media Controls: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of a facility, and the movement of these items within the facility.

164.310(d)(2)(i) Have you implemented policies and procedures to address final disposition of EPHI, and/or hardware or electronic media on which it is stored? (R)	Compliant
164.310(d)(2)(ii) Have you implemented procedures for removal of EPHI from electronic media before the media are available for reuse? (R)	Compliant
164.310(d)(2)(iii) Do you maintain a record of the movements of hardware and electronic media and the person responsible for its movement? (A)	Compliant
164.310(d)(2)(iv) Do you create a retrievable, exact copy of EPHI, when needed, before movement of equipment? (A)	Compliant

Technical Safeguards

100%

164.312(a)(1) Access Controls: Implement technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights as	Compliant

specified in Sec. 164.308(a)(4).	
164.312(a)(2)(i) Have you assigned a unique name and/or number for identifying and tracking user identity? (R)	Compliant
164.312(a)(2)(ii) Have you established (and implemented as needed) procedures for obtaining for obtaining necessary EPHI during and	Compliant
emergency? (R)	Compliant
164.312(a)(2)(iii) Have you implemented procedures that terminate an electronic session after a predetermined time of inactivity? (A)	Compliant
164.312(a)(2)(iv) Have you implemented a mechanism to encrypt and decrypt EPHI? (A)	Compliant
164.312(b) Have you implemented Audit Controls, hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI? (R)	Compliant
164.312(c)(1) Integrity: Implement policies and procedures to protect EPHI from improper alteration or destruction.	
164.312(c)(2) Have you implemented electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner? (A)	Compliant
164.312(d) Have you implemented Person or Entity Authentication procedures to verify that a person or entity seeking access EPHI is the one claimed? (R)	Compliant
164.312(e)(1) Transmission Security: Implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network.	
164.312(e)(2)(i) Have you implemented security measures to ensure that electronically transmitted EPHI is not improperly modified	Compliant
without detection until disposed of? (A)	Compliant
164.312(e)(2)(ii) Have you implemented a mechanism to encrypt EPHI whenever deemed appropriate? (A)	Compliant

Completion

Comments/Recommendations

- Conduct a general review of the formal sanctions for those who violate our organization's security policies and procedures.
- To reiterate, our information security and privacy compliance officers are expected to provide reports and documentation regarding the Q2 and Q3 records reviews before the end of Q4 so that we can assess what didn't go well and address such concerns to avoid in the future.

Name and Signature of Auditor

Shay Park
05.05.2023 19:55 PST

Media summary

Formal Sanctions - Violations on Security SOPs.pdf

FY22-23 Q2 Records Review - Timeline & Results.pdf

FY22-23 Q3 Records Review - Timeline & Results.pdf