HIPAA Readiness report for AI Health Studio LLC

Generated on 03 November 2026

Report summary

This report provides a summary of AI Health Studio LLC's readiness posture for HIPAA compliance as of 3rd November 2026. Sprinto continuously monitors the security and readiness posture of AI Health Studio LLC to ensure you have a transparent view into how they have setup Sprinto to meet industry standards. Below is a list of controls implemented by the organization to meet the compliance requirements. Sprinto achieves this by connecting to the systems, tools and policies of the company, and running continuous checks to determine the health of the controls.

164.310

Physical safeguards

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.

INTERNAL CONTROLS AND CHECKS

Control **SDC 381**

Entity has documented policies and procedures to manage physical and environmental security.

MONITORED via 2 checks

Physical and Environmental Security Procedure
Physical & Environmental Security Policy

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

MONITORED via 2 checks

Vendor risk assessment should be conducted periodically
Vendor Management Policy

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

MONITORED via 3 checks

Vendor risk assessment should be reviewed by senior management
Vendor Management Policy
Vendor Management Procedure

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

MONITORED via 1 check

Vendor Management Policy

164.310(a)(2)(i)

Contingency operations: Establish (and implement 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.

INTERNAL CONTROLS AND CHECKS

Control **SDC 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.

MONITORED via 2 checks

Incident Management Procedure
Incident Management Policy

Control **SDC 392**

Entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident

MONITORED via 2 checks

Business Continuity Plan
Business Continuity & Disaster Recovery Policy

Control **SDC 393**

Entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.

MONITORED via 2 checks

Business Continuity Plan
Business Continuity & Disaster Recovery Policy

164.310(a)(2)(ii)

Facility security plan: Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

INTERNAL CONTROLS AND CHECKS

Control **SDC 381**

Entity has documented policies and procedures to manage physical and environmental security.

MONITORED via 2 checks

Physical and Environmental Security Procedure
Physical & Environmental Security Policy

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

MONITORED via 2 checks

Vendor risk assessment should be conducted periodically
Vendor Management Policy

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

MONITORED via 3 checks

Vendor risk assessment should be reviewed by senior management
Vendor Management Policy
Vendor Management Procedure

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

MONITORED via 1 check

Vendor Management Policy

164.310(a)(2)(iii)

Access control and validation procedures: Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

MONITORED via 2 checks

Vendor risk assessment should be conducted periodically
Vendor Management Policy

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

MONITORED via 3 checks

Vendor risk assessment should be reviewed by senior management
Vendor Management Policy
Vendor Management Procedure

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

MONITORED via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control SDC 68

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

MONITORED via 1 check

Vendor Management Policy

Control SDC 33

Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.

MONITORED via 2 checks

Access Control Procedure
Access Control Policy

Control SDC 34

Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.

MONITORED via 6 checks

User access to critical system should be validated by roles
Role based access should be setup
HR Security Procedure
Access Control Procedure
HR Security Policy
Access Control Policy

Control SDC 42

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

MONITORED via 4 checks

Access to critical systems should be reviewed

Users of critical system should be identified
Access Control Procedure
Access Control Policy

Control SDC 43

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

MONITORED via 4 checks

Access to critical systems should be reviewed
Users of critical system should be identified
Access Control Procedure
Access Control Policy

164.310(a)(2)(iv)

Maintenance records: Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

INTERNAL CONTROLS AND CHECKS

Control SDC 48

Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.

MONITORED via 1 check

Media Disposal Policy

Control SDC 381

Entity has documented policies and procedures to manage physical and environmental security.

MONITORED via 2 checks

Physical and Environmental Security Procedure
Physical & Environmental Security Policy

Control SDC 31

Entity has documented a set of policies and procedures that establish expected behavior with regard to the Company’s control environment.

MONITORED via 1 check

Org policy should be defined

164.310(b)

Workstation use: Implement 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.

INTERNAL CONTROLS AND CHECKS

Control SDC 104

Entity has documented policies and procedures for endpoint security and related controls.

MONITORED via 3 checks

Endpoint Security Policy
Asset Management Policy
Asset Management Procedure

Control SDC 44

Where applicable, Entity ensures that endpoints with access to critical servers or data must be protected by malware-protection software.

MONITORED via 5 checks

Staff devices should have antivirus running
Endpoint Security Policy
Asset Management Policy
Physical and Environmental Security Procedure
Asset Management Procedure

Control SDC 45

Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.

MONITORED via 2 checks

Staff devices should have disk encryption enabled
Endpoint Security Policy

Control **SDC 46**

Entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.

MONITORED via 5 checks

Staff devices should have OS updated
Endpoint Security Policy
Asset Management Policy
Physical and Environmental Security Procedure
Asset Management Procedure

Control **SDC 47**

Entity ensures that endpoints with access to critical servers or data are configured to auto-screen-lock after 15 minutes of inactivity.

MONITORED via 3 checks

Staff devices health should be monitored regularly
Staff devices should have screen lock enabled
Endpoint Security Policy

Control **SDC 48**

Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.

MONITORED via 1 check

Media Disposal Policy

164.310(c)

Workstation security: Covered entities should implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.

INTERNAL CONTROLS AND CHECKS

Control **SDC 44**

Where applicable, Entity ensures that endpoints with access to critical servers or data must be protected by malware-protection software.

MONITORED via 5 checks

Staff devices should have antivirus running
Endpoint Security Policy
Asset Management Policy
Physical and Environmental Security Procedure
Asset Management Procedure

Control **SDC 45**

Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.

MONITORED via 2 checks

Staff devices should have disk encryption enabled
Endpoint Security Policy

Control **SDC 46**

Entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.

MONITORED via 5 checks

Staff devices should have OS updated
Endpoint Security Policy
Asset Management Policy
Physical and Environmental Security Procedure
Asset Management Procedure

Control **SDC 47**

Entity ensures that endpoints with access to critical servers or data are configured to auto-screen-lock after 15 minutes of inactivity.

MONITORED via 3 checks

Staff devices health should be monitored regularly
Staff devices should have screen lock enabled
Endpoint Security Policy

Control **SDC 48**

Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.

MONITORED via 1 check

Media Disposal Policy

Control **SDC 104**

Entity has documented policies and procedures for endpoint security and related controls.

MONITORED via 3 checks

Endpoint Security Policy
Asset Management Policy
Asset Management Procedure

164.310(d)(1)

Device and media control: 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.

INTERNAL CONTROLS AND CHECKS

Control **SDC 48**

Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.

MONITORED via 1 check

Media Disposal Policy

Control **SDC 105**

Entity establishes guidelines for acceptable and unacceptable technology usage behaviors, including outlining consequences for unacceptable actions.

MONITORED via 1 check

Acceptable Usage Policy

Control **SDC 382**

Entity has documented policy and procedures for physical and/or logical labeling of information via documented policy for data classification.

MONITORED via 1 check

Data Classification Policy

Control **SDC 70**

Entity performs physical and/or logical labeling of information systems as per the guidelines documented policy defined for data classification

MONITORED via 1 check

Data Classification Policy

Control **SDC 69**

Entity has a documented Information Security Policy that governs the confidentiality, integrity, and availability of information systems

MONITORED via 1 check

Information Security Policy

Control **SDC 390**

Entity develops, documents, and maintains an inventory of organizational endpoint systems, including all necessary information to achieve accountability.

MONITORED via 3 checks

Staff devices health should be monitored regularly

Endpoint Security Policy

Asset Management Procedure

164.310(d)(2)(i)

Disposal: Implement policies and procedures to address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored.

INTERNAL CONTROLS AND CHECKS

Control **SDC 48**

Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.

MONITORED via 1 check

Media Disposal Policy

164.310(d)(2)(ii)

Media re-use: Implement procedures for removal of ePHI from electronic media before the media are made available for re-use. Ensure that ePHI previously stored on electronic media cannot be accessed and reused. Identify removable media and their use. Ensure that ePHI is removed from reusable media before they are used to record new information.

INTERNAL CONTROLS AND CHECKS

Control **SDC 70**

Entity performs physical and/or logical labeling of information systems as per the guidelines documented policy defined for data classification

MONITORED via 1 check

Data Classification Policy

Control **SDC 382**

Entity has documented policy and procedures for physical and/or logical labeling of information via documented policy for data classification.

MONITORED via 1 check

Data Classification Policy

164.310(d)(2)(iii)

Accountability: Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

INTERNAL CONTROLS AND CHECKS

Control **SDC 70**

Entity performs physical and/or logical labeling of information systems as per the guidelines documented policy defined for data classification

MONITORED via 1 check

Data Classification Policy

Control **SDC 71**

Entity has a documented policy outlining guidelines for the disposal and retention of information.

MONITORED via 1 check

Data Retention Policy

Control **SDC 72**

Entity has a documented policy and procedures to provide guidelines for Data Protection which includes staff members' responsibilities with handling personal data as per the company's regulatory requirements

MONITORED via 1 check

Data Protection Policy

Control **SDC 48**

Entity has a documented policy that provides guidance on decommissioning of information assets that contain classified information.

MONITORED via 1 check

Media Disposal Policy

Control SDC 104

Entity has documented policies and procedures for endpoint security and related controls.

MONITORED via 3 checks

Endpoint Security Policy
Asset Management Policy
Asset Management Procedure

164.310(d)(2)(iv)

Data backup and storage: Create a retrievable, exact copy of ePHI, when needed, before movement of equipment.

INTERNAL CONTROLS AND CHECKS

Control SDC 58

Entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal

MONITORED via 2 checks

Operation Security Policy
Operations Security Procedure

Control SDC 59

Entity backs up relevant user and system data regularly to meet recovery time and recovery point objectives and verifies the integrity of these backups.

MONITORED via 5 checks

Backup should be enabled on production database
Versioning should be enabled for storage assets
Operation Security Policy
Business Continuity Plan
Operations Security Procedure

164.312

Technical safeguards

164.312(a)(1)

Access control: 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 specified in §164.308(a)(4) □Information Access Management].

INTERNAL CONTROLS AND CHECKS

Control **SDC 33**

Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.

MONITORED via 2 checks

Access Control Procedure
Access Control Policy

Control **SDC 34**

Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.

MONITORED via 6 checks

User access to critical system should be validated by roles
Role based access should be setup
HR Security Procedure
Access Control Procedure
HR Security Policy
Access Control Policy

Control **SDC 35**

Entity ensures logical access that is no longer required in the event of termination is made inaccessible in a timely manner.

MONITORED via 4 checks

HR Security Procedure
Access Control Procedure

HR Security Policy
Access Control Policy

Control **SDC 37**

Entity ensures that access to the production databases is restricted to only those individuals who require such access to perform their job functions.

MONITORED via 5 checks

Access to critical systems should be reviewed
Policies should be attached to groups and should not be attached to users
Users of critical system should be identified
Access Control Procedure
Access Control Policy

Control **SDC 38**

Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.

MONITORED via 1 check

Public access for infra assets should be restricted

Control **SDC 39**

Entity requires that all staff members with access to any critical system be protected with a secure login mechanism such as Multifactor-authentication.

MONITORED via 3 checks

Critical systems should be protected with a secure login mechanism
Access Control Procedure
Access Control Policy

DECLARED via 1 check

Access should be protected with secure login mechanism

Control **SDC 42**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

MONITORED via 4 checks

Access to critical systems should be reviewed
Users of critical system should be identified
Access Control Procedure
Access Control Policy

Control SDC 43

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

MONITORED via 4 checks

Access to critical systems should be reviewed
Users of critical system should be identified
Access Control Procedure
Access Control Policy

164.312(a)(2)(i)

Unique user identification: Assign a unique name and/or number for identifying and tracking user identity. Ensure that system activity can be traced to a specific user. Ensure that the necessary data is available in the system logs to support audit and other related business functions.

INTERNAL CONTROLS AND CHECKS

Control SDC 39

Entity requires that all staff members with access to any critical system be protected with a secure login mechanism such as Multifactor-authentication.

MONITORED via 3 checks

Critical systems should be protected with a secure login mechanism
Access Control Procedure
Access Control Policy

DECLARED via 1 check

Access should be protected with secure login mechanism

Control SDC 37

Entity ensures that access to the production databases is restricted to only those individuals who require such access to perform their job functions.

MONITORED via 5 checks

Access to critical systems should be reviewed
Policies should be attached to groups and should not be attached to users
Users of critical system should be identified
Access Control Procedure
Access Control Policy

Control **SDC 38**

Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.

MONITORED via 1 check

Public access for infra assets should be restricted

Control **SDC 42**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

MONITORED via 4 checks

Access to critical systems should be reviewed
Users of critical system should be identified
Access Control Procedure
Access Control Policy

Control **SDC 43**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

MONITORED via 4 checks

Access to critical systems should be reviewed
Users of critical system should be identified
Access Control Procedure
Access Control Policy

164.312(a)(2)(ii)

Emergency access procedure: Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.

INTERNAL CONTROLS AND CHECKS

Control **SDC 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.

MONITORED via 2 checks

Incident Management Procedure
Incident Management Policy

Control **SDC 392**

Entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident

MONITORED via 2 checks

Business Continuity Plan
Business Continuity & Disaster Recovery Policy

Control **SDC 393**

Entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.

MONITORED via 2 checks

Business Continuity Plan
Business Continuity & Disaster Recovery Policy

164.312(a)(2)(iii)

Automatic logoff: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

INTERNAL CONTROLS AND CHECKS

Control SDC 47

Entity ensures that endpoints with access to critical servers or data are configured to auto-screen-lock after 15 minutes of inactivity.

MONITORED via 3 checks

Staff devices health should be monitored regularly
Staff devices should have screen lock enabled
Endpoint Security Policy

Control SDC 109

Entity ensures infrastructure cloud provider login sessions are terminated after a defined length of time.

MONITORED via 2 checks

Access Control Procedure
Access Control Policy

DECLARED via 1 check

Login Session Termination

164.312(a)(2)(iv)

Encryption and decryption: Implement a mechanism to encrypt and decrypt ePHI.

INTERNAL CONTROLS AND CHECKS

Control SDC 45

Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.

MONITORED via 2 checks

Staff devices should have disk encryption enabled
Endpoint Security Policy

Control SDC 49

Entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.

MONITORED via 4 checks

Data at rest should be encrypted
Encryption Policy
Asset Management Policy
Asset Management Procedure

Control **SDC 51**

Entity has set up processes to utilize standard encryption methods, including HTTPS with the TLS algorithm, to keep transmitted data confidential.

MONITORED via 1 check

Production systems should be secured with HTTPS

Control **SDC 106**

Entity has a documented policy to manage encryption and cryptographic protection controls.

MONITORED via 1 check

Encryption Policy

164.312(b)

Audit controls: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

INTERNAL CONTROLS AND CHECKS

Control **SDC 61**

Entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats

MONITORED via 1 check

Threat detection system should be enabled

Control **SDC 62**

Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.

MONITORED via 4 checks

Health of production infrastructure should be monitored
Errors on production infrastructure should be monitored
Operation Security Policy
Operations Security Procedure

Control **SDC 394**

Entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.

MONITORED via 3 checks

Audit logs should exist
Operation Security Policy
Operations Security Procedure

164.312(c)(1)

Integrity: Implement policies and procedures to protect ePHI from improper alteration or destruction.

INTERNAL CONTROLS AND CHECKS

Control **SDC 71**

Entity has a documented policy outlining guidelines for the disposal and retention of information.

MONITORED via 1 check

Data Retention Policy

Control **SDC 72**

Entity has a documented policy and procedures to provide guidelines for Data Protection which includes staff members' responsibilities with handling personal data as per the company's regulatory requirements

MONITORED via 1 check

Data Protection Policy

Control SDC 70

Entity performs physical and/or logical labeling of information systems as per the guidelines documented policy defined for data classification

MONITORED via 1 check

Data Classification Policy

164.312(c)(2)

Mechanisms to authenticate ePHI Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.

INTERNAL CONTROLS AND CHECKS

Control SDC 61

Entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats

MONITORED via 1 check

Threat detection system should be enabled

Control SDC 63

Entity identifies vulnerabilities on the company platform through an annual penetration testing exercise conducted by a qualified third-party service provider.

MONITORED via 1 check

VAPT exercise should be conducted annually

Control SDC 62

Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.

MONITORED via 4 checks

Health of production infrastructure should be monitored
Errors on production infrastructure should be monitored
Operation Security Policy
Operations Security Procedure

Control **SDC 56**

Entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.

MONITORED via 1 check

Vulnerability should be closed in SLA

Control **SDC 55**

Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.

MONITORED via 2 checks

Vulnerability should be closed in SLA
Vulnerability scanner should be enabled

164.312(d)

Person or entity authentication: Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.

INTERNAL CONTROLS AND CHECKS

Control **SDC 33**

Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.

MONITORED via 2 checks

Access Control Procedure
Access Control Policy

Control **SDC 34**

Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.

MONITORED via 6 checks

User access to critical system should be validated by roles
Role based access should be setup
HR Security Procedure
Access Control Procedure
HR Security Policy
Access Control Policy

Control **SDC 35**

Entity ensures logical access that is no longer required in the event of termination is made inaccessible in a timely manner.

MONITORED via 4 checks

HR Security Procedure
Access Control Procedure
HR Security Policy
Access Control Policy

Control **SDC 37**

Entity ensures that access to the production databases is restricted to only those individuals who require such access to perform their job functions.

MONITORED via 5 checks

Access to critical systems should be reviewed
Policies should be attached to groups and should not be attached to users
Users of critical system should be identified
Access Control Procedure
Access Control Policy

Control **SDC 38**

Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.

MONITORED via 1 check

Public access for infra assets should be restricted

Control **SDC 39**

Entity requires that all staff members with access to any critical system be protected with a secure login mechanism such as Multifactor-authentication.

MONITORED via 3 checks

Critical systems should be protected with a secure login mechanism
Access Control Procedure
Access Control Policy

DECLARED via 1 check

Access should be protected with secure login mechanism

Control **SDC 42**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

MONITORED via 4 checks

Access to critical systems should be reviewed
Users of critical system should be identified
Access Control Procedure
Access Control Policy

Control **SDC 43**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

MONITORED via 4 checks

Access to critical systems should be reviewed
Users of critical system should be identified
Access Control Procedure
Access Control Policy

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.

INTERNAL CONTROLS AND CHECKS

Control **SDC 70**

Entity performs physical and/or logical labeling of information systems as per the guidelines documented policy defined for data classification

MONITORED via 1 check

Data Classification Policy

Control **SDC 69**

Entity has a documented Information Security Policy that governs the confidentiality, integrity, and availability of information systems

MONITORED via 1 check

Information Security Policy

Control **SDC 106**

Entity has a documented policy to manage encryption and cryptographic protection controls.

MONITORED via 1 check

Encryption Policy

Control **SDC 49**

Entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.

MONITORED via 4 checks

Data at rest should be encrypted
Encryption Policy
Asset Management Policy
Asset Management Procedure

Control **SDC 51**

Entity has set up processes to utilize standard encryption methods, including HTTPS with the TLS algorithm, to keep transmitted data confidential.

MONITORED via 1 check

Production systems should be secured with HTTPS

Control **SDC 45**

Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.

MONITORED via 2 checks

Staff devices should have disk encryption enabled
Endpoint Security Policy

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

DECLARED via 1 check

Records of Processing Activities (ROPA) & Data flow map

164.312(e)(2)(i)

Integrity controls: Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.

INTERNAL CONTROLS AND CHECKS

Control **SDC 106**

Entity has a documented policy to manage encryption and cryptographic protection controls.

MONITORED via 1 check

Encryption Policy

Control **SDC 7**

Entity provides information security and privacy training to staff that is relevant to their job function.

MONITORED via 2 checks

Security training provider should be configured
HR Security Policy

Control SDC 6

Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.

MONITORED via 1 check

Policies should be acknowledged by onboarded staff

164.312(e)(2)(ii)

Encryption: Implement a mechanism to encrypt ePHI whenever deemed appropriate.

INTERNAL CONTROLS AND CHECKS

Control SDC 45

Where applicable, Entity ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.

MONITORED via 2 checks

Staff devices should have disk encryption enabled
Endpoint Security Policy

Control SDC 49

Entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.

MONITORED via 4 checks

Data at rest should be encrypted
Encryption Policy
Asset Management Policy
Asset Management Procedure

Control SDC 51

Entity has set up processes to utilize standard encryption methods, including HTTPS with the TLS algorithm, to keep transmitted data confidential.

MONITORED via 1 check

Production systems should be secured with HTTPS

Control SDC 106

Entity has a documented policy to manage encryption and cryptographic protection controls.

MONITORED via 1 check

Encryption Policy

164.316

Policies, procedures and documentation requirements

164.316(a)

Policies and Procedures: Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in 164.306(b)(2)(i), (ii), (iii), and (iv) [the Security Standards: General Rules, Flexibility of Approach]. This standard is not to be construed to permit or excuse an action that violates any other standard. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.

INTERNAL CONTROLS AND CHECKS

Control SDC 24

Entity's Senior Management reviews and approves all company policies annually.

MONITORED via 1 check

Policies should be reviewed by senior management

Control SDC 31

Entity has documented a set of policies and procedures that establish expected behavior with regard to the Company’s control environment.

MONITORED via 1 check

Org policy should be defined

Control SDC 111

Entity ensures that all policy documents are retained for at least (6) years from creation.

MONITORED via 1 check

Org policy should be defined

164.316(b)(1)(i)

Documentation: Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) if an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.

INTERNAL CONTROLS AND CHECKS

Control SDC 24

Entity's Senior Management reviews and approves all company policies annually.

MONITORED via 1 check

Policies should be reviewed by senior management

Control SDC 31

Entity has documented a set of policies and procedures that establish expected behavior with regard to the Company’s control environment.

MONITORED via 1 check

Org policy should be defined

164.316(b)(1)(ii)

Documentation: if an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.

INTERNAL CONTROLS AND CHECKS

Control **SDC 31**

Entity has documented a set of policies and procedures that establish expected behavior with regard to the Company’s control environment.

MONITORED via 1 check

Org policy should be defined

Control **SDC 24**

Entity's Senior Management reviews and approves all company policies annually.

MONITORED via 1 check

Policies should be reviewed by senior management

164.316(b)(2)(i)

Time Limit: Retain the documentation required by paragraph (b) (1) of this section for 6 years for the date of its creation or the date when it last was in effect, whichever is later.

INTERNAL CONTROLS AND CHECKS

Control **SDC 71**

Entity has a documented policy outlining guidelines for the disposal and retention of information.

MONITORED via 1 check

Data Retention Policy

Control **SDC 111**

Entity ensures that all policy documents are retained for at least (6) years from creation.

MONITORED via 1 check

Org policy should be defined

164.316(b)(2)(ii)

Availability: Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains

INTERNAL CONTROLS AND CHECKS

Control **SDC 6**

Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.

MONITORED via 1 check

Policies should be acknowledged by onboarded staff

Control **SDC 12**

Entity has established procedures for staff to acknowledge applicable company policies periodically.

MONITORED via 1 check

Policies should be acknowledged by onboarded staff

Control **SDC 31**

Entity has documented a set of policies and procedures that establish expected behavior with regard to the Company’s control environment.

MONITORED via 1 check

Org policy should be defined

Control **SDC 24**

Entity's Senior Management reviews and approves all company policies annually.

MONITORED via 1 check

Policies should be reviewed by senior management

164.316(b)(2)(iii)

Updates: Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the ePHI.

INTERNAL CONTROLS AND CHECKS

Control **SDC 112**

Entity has documented guidelines on notifying customers and other stakeholders in case of a breach.

MONITORED via 3 checks

Data Breach Notification Policy
PHI Data breach Notification Procedure
Personal Data Breach Notification Procedure

164.410

Notification by a business associate in the case of breach of unsecured Protected Health Information (PHI)

164.410(a)(1)

A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach.

INTERNAL CONTROLS AND CHECKS

Control **SDC 112**

Entity has documented guidelines on notifying customers and other stakeholders in case of a breach.

MONITORED via 3 checks

Data Breach Notification Policy
PHI Data breach Notification Procedure
Personal Data Breach Notification Procedure

Control SDC 113

Entity conducts risk assessment of suspected data breaches and any significant data breaches are notified to all affected parties without unreasonable delay.

MONITORED via 3 checks

Incidents should be investigated based on severity
Incident Management Procedure
Incident Management Policy

Control SDC 53

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.

MONITORED via 2 checks

Incident Management Procedure
Incident Management Policy

Control SDC 54

Entity maintains a record of information security incidents, its investigation, and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.

MONITORED via 1 check

Incidents should be investigated based on severity

164.410(a)(2)

For the purposes of paragraph (1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the federal common law of agency).

INTERNAL CONTROLS AND CHECKS

Control **SDC 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.

MONITORED via 2 checks

Incident Management Procedure
Incident Management Policy

Control **SDC 112**

Entity has documented guidelines on notifying customers and other stakeholders in case of a breach.

MONITORED via 3 checks

Data Breach Notification Policy
PHI Data breach Notification Procedure
Personal Data Breach Notification Procedure

Control **SDC 113**

Entity conducts risk assessment of suspected data breaches and any significant data breaches are notified to all affected parties without unreasonable delay.

MONITORED via 3 checks

Incidents should be investigated based on severity
Incident Management Procedure
Incident Management Policy

164.410(b)

Except as provided in §164.412, a business associate shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach.

INTERNAL CONTROLS AND CHECKS

Control **SDC 6**

Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.

MONITORED via 1 check

Policies should be acknowledged by onboarded staff

Control **SDC 12**

Entity has established procedures for staff to acknowledge applicable company policies periodically.

MONITORED via 1 check

Policies should be acknowledged by onboarded staff

Control **SDC 112**

Entity has documented guidelines on notifying customers and other stakeholders in case of a breach.

MONITORED via 3 checks

Data Breach Notification Policy
PHI Data breach Notification Procedure
Personal Data Breach Notification Procedure

Control **SDC 113**

Entity conducts risk assessment of suspected data breaches and any significant data breaches are notified to all affected parties without unreasonable delay.

MONITORED via 3 checks

Incidents should be investigated based on severity
Incident Management Procedure
Incident Management Policy

Control **SDC 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.

MONITORED via 2 checks

Incident Management Procedure
Incident Management Policy

Control SDC 54

Entity maintains a record of information security incidents, its investigation, and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.

MONITORED via 1 check

Incidents should be investigated based on severity

164.410(c)(1)

The notification required by paragraph (a) of this section shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been accessed, acquired, used or disclosure during the breach.

INTERNAL CONTROLS AND CHECKS

Control SDC 53

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.

MONITORED via 2 checks

Incident Management Procedure
Incident Management Policy

Control SDC 112

Entity has documented guidelines on notifying customers and other stakeholders in case of a breach.

MONITORED via 3 checks

Data Breach Notification Policy
PHI Data breach Notification Procedure
Personal Data Breach Notification Procedure

Control SDC 113

Entity conducts risk assessment of suspected data breaches and any significant data breaches are notified to all affected parties without unreasonable delay.

MONITORED via 3 checks

Incidents should be investigated based on severity
Incident Management Procedure
Incident Management Policy

164.410(c)(2)

A business associate shall provide the covered entity with any other information that the covered entity is required to include in the notification to the individual under §164.404(c) at the time of the notification required by paragraph (a) of this section or promptly thereafter as information becomes available.

INTERNAL CONTROLS AND CHECKS

Control **SDC 112**

Entity has documented guidelines on notifying customers and other stakeholders in case of a breach.

MONITORED via 3 checks

Data Breach Notification Policy
PHI Data breach Notification Procedure
Personal Data Breach Notification Procedure

Control **SDC 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.

MONITORED via 2 checks

Incident Management Procedure
Incident Management Policy

164.308

Administrative safeguards

164.308(a)(1)(i)

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

INTERNAL CONTROLS AND CHECKS

Control **SDC 433**

Entity has documented policy and procedures which provides guidance on integrating privacy principles into the design process that help in complying with privacy regulations.

MONITORED via 1 check

Privacy By Design Policy

Control **SDC 15**

Entity has provided information to employees, via various Information Security Policies/procedures, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.

MONITORED via 1 check

Information Security Policy

Control **SDC 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.

MONITORED via 2 checks

Incident Management Procedure
Incident Management Policy

Control **SDC 112**

Entity has documented guidelines on notifying customers and other stakeholders in case of a breach.

MONITORED via 3 checks

Data Breach Notification Policy
PHI Data breach Notification Procedure
Personal Data Breach Notification Procedure

Control **SDC 100**

Entity ensures that customer data used in non-Production environments requires the same level of protection as the production environment.

MONITORED via 3 checks

Critical Infrastructure assets should be identified
Asset Management Policy
Asset Management Procedure

Control **SDC 104**

Entity has documented policies and procedures for endpoint security and related controls.

MONITORED via 3 checks

Endpoint Security Policy
Asset Management Policy
Asset Management Procedure

Control **SDC 108**

Entity uses Sprinto, a continuous monitoring system, to alert the security team to update the access levels of team members whose roles have changed.

MONITORED via 3 checks

Access to critical systems should be reviewed
Access Control Procedure
Access Control Policy

164.308(a)(3)(i)

Workforce security: Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under the Information Access Management standard and to prevent those who do not have appropriate access from obtaining access to ePHI. Policies and procedures should include Authorization and/or Supervision procedures, Workforce Clearance Procedure, and Termination Procedures.

INTERNAL CONTROLS AND CHECKS

Control **SDC 1**

Entity has a documented policy to define behavioral standards and acceptable business conduct.

MONITORED via 1 check

Code of Business Conduct Policy

Control **SDC 2**

Entity maintains an organizational structure to define authorities, facilitate information flow and establish responsibilities.

MONITORED via 5 checks

Org chart should be maintained
HR Security Procedure
Access Control Procedure
HR Security Policy
Access Control Policy

Control **SDC 3**

Entity has established procedures to communicate with staff about their roles and responsibilities.

MONITORED via 3 checks

Organization roles and JDs should be validated
HR Security Procedure
HR Security Policy

Control **SDC 4**

Entity has procedures to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.

MONITORED via 2 checks

HR Security Procedure
HR Security Policy

Control **SDC 9**

Entity requires that all employees in client serving, IT, Engineering, and Information Security roles are periodically evaluated regarding their job responsibilities.

MONITORED via 2 checks

HR Security Procedure
HR Security Policy

DECLARED via 1 check

Staff Performance Evaluations

Control **SDC 33**

Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.

MONITORED via 2 checks

Access Control Procedure
Access Control Policy

Control **SDC 34**

Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.

MONITORED via 6 checks

User access to critical system should be validated by roles
Role based access should be setup
HR Security Procedure
Access Control Procedure
HR Security Policy
Access Control Policy

Control **SDC 35**

Entity ensures logical access that is no longer required in the event of termination is made inaccessible in a timely manner.

MONITORED via 4 checks

HR Security Procedure
Access Control Procedure
HR Security Policy
Access Control Policy

Control **SDC 37**

Entity ensures that access to the production databases is restricted to only those individuals who require such access to perform their job functions.

MONITORED via 5 checks

Access to critical systems should be reviewed
Policies should be attached to groups and should not be attached to users
Users of critical system should be identified
Access Control Procedure
Access Control Policy

Control **SDC 38**

Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.

MONITORED via 1 check

Public access for infra assets should be restricted

Control **SDC 39**

Entity requires that all staff members with access to any critical system be protected with a secure login mechanism such as Multifactor-authentication.

MONITORED via 3 checks

Critical systems should be protected with a secure login mechanism
Access Control Procedure
Access Control Policy

DECLARED via 1 check

Access should be protected with secure login mechanism

Control **SDC 42**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

MONITORED via 4 checks

Access to critical systems should be reviewed
Users of critical system should be identified
Access Control Procedure
Access Control Policy

Control **SDC 43**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

MONITORED via 4 checks

- Access to critical systems should be reviewed
- Users of critical system should be identified
- Access Control Procedure
- Access Control Policy

164.308(a)(6)(ii)

Response and reporting: Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.

INTERNAL CONTROLS AND CHECKS

Control **SDC 1104**

Entity has documented guidelines on notifying customers and other stakeholders in case of a PHI breach.

MONITORED via 58 checks

- Change management repos should be classified
- Changes to production code should be reviewed by peers
- Change requests should be reviewed by peers
- Compliance program manager should be assigned
- Information security officer should be assigned
- Infrastructure operations person should be assigned
- Infosec training should be completed by onboarded staff
- Policies should be acknowledged by onboarded staff
- Org chart should be maintained
- People operations person should be assigned
- Staff should periodically complete security training
- Org policy should be defined
- Privacy officer should be assigned
- Risk assessment should be conducted periodically
- Organization roles and JDs should be validated
- Security training provider should be configured
- Senior management should be assigned
- Staff devices health should be monitored regularly
- Vendor risk assessment should be conducted periodically
- System Description

Privacy By Design Policy
SDLC Procedure
Compliance Procedure
HR Security Procedure
Data Classification Policy
Media Disposal Policy
Compliance Policy
Data Retention Policy
Encryption Policy
Communications & Network Security Policy
Endpoint Security Policy
Cardholder Data Management Policy
Operation Security Policy
Incident Management Procedure
Business Continuity Plan
Vendor Management Policy
Code of Business Conduct Policy
Data Breach Notification Policy
Operations Security Procedure
Business Continuity & Disaster Recovery Policy
PHI Data breach Notification Procedure
Asset Management Policy
Personal Data Breach Notification Procedure
Incident Management Policy
Network Security Procedure
Physical and Environmental Security Procedure
Organization of Information Security Policy
System Acquisition and Development Lifecycle Policy
Access Control Procedure
Asset Management Procedure
Vendor Management Procedure
Data Protection Policy
HR Security Policy
Information Security Policy
Acceptable Usage Policy
Physical & Environmental Security Policy
Risk Assessment & Management Policy
Access Control Policy

DECLARED via 1 check

Staff Performance Evaluations

Control **SDC 15**

Entity has provided information to employees, via various Information Security Policies/procedures, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.

MONITORED via 1 check

Information Security Policy

Control **SDC 16**

Entity has provided information to customers on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the Entity in the event there are problems.

MONITORED via 1 check

Customer support page (Contact Us) should be available

Control **SDC 54**

Entity maintains a record of information security incidents, its investigation, and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.

MONITORED via 1 check

Incidents should be investigated based on severity

Control **SDC 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.

MONITORED via 2 checks

Incident Management Procedure
Incident Management Policy

Control **SDC 112**

Entity has documented guidelines on notifying customers and other stakeholders in case of a breach.

MONITORED via 3 checks

Data Breach Notification Policy
PHI Data breach Notification Procedure
Personal Data Breach Notification Procedure

164.308(a)(1)(ii)(A)

Risk analysis: 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 or business associate.

INTERNAL CONTROLS AND CHECKS

Control **SDC 18**

Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.

MONITORED via 2 checks

Risk assessment should be conducted periodically
Risk Assessment & Management Policy

Control **SDC 67**

Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the Entity's service commitments and system requirements

MONITORED via 1 check

Risk Assessment & Management Policy

Control **SDC 391**

Entity has a documented policy and procedures to establish guidelines for managing technical vulnerabilities.

MONITORED via 2 checks

Operation Security Policy
Operations Security Procedure

164.308(a)(1)(ii)(B)

Risk management: Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a). Factors identified in §164.306 include: · The size, complexity, capability of the covered entity; · The covered entity’s technical infrastructure; · The costs of security measures; and · The probability and criticality of potential risks to ePHI

INTERNAL CONTROLS AND CHECKS

Control **SDC 18**

Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.

MONITORED via 2 checks

Risk assessment should be conducted periodically
Risk Assessment & Management Policy

Control **SDC 67**

Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the Entity's service commitments and system requirements

MONITORED via 1 check

Risk Assessment & Management Policy

Control **SDC 5**

Entity has established procedures to perform security risk screening of individuals before authorizing access.

MONITORED via 2 checks

HR Security Procedure
HR Security Policy

164.308(a)(1)(ii)(C)

Sanction policy: Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

INTERNAL CONTROLS AND CHECKS

Control **SDC 6**

Entity has established procedures for new staff to acknowledge applicable company policies as a part of their onboarding.

MONITORED via 1 check

Policies should be acknowledged by onboarded staff

Control **SDC 12**

Entity has established procedures for staff to acknowledge applicable company policies periodically.

MONITORED via 1 check

Policies should be acknowledged by onboarded staff

Control **SDC 31**

Entity has documented a set of policies and procedures that establish expected behavior with regard to the Company’s control environment.

MONITORED via 1 check

Org policy should be defined

164.308(a)(1)(ii)(D)

Information system activity review: Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

INTERNAL CONTROLS AND CHECKS

Control **SDC 33**

Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.

MONITORED via 2 checks

Access Control Procedure

Access Control Policy

Control **SDC 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.

MONITORED via 2 checks

Incident Management Procedure
Incident Management Policy

Control SDC 54

Entity maintains a record of information security incidents, its investigation, and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.

MONITORED via 1 check

Incidents should be investigated based on severity

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 covered entity or business associate.

INTERNAL CONTROLS AND CHECKS

Control SDC 22

Entity's Senior Management assigns the role of Information Security Officer who is delegated to centrally manage, coordinate, develop, implement, and maintain an enterprise-wide cybersecurity and privacy program.

MONITORED via 1 check

Information security officer should be assigned

Control SDC 25

Entity's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.

MONITORED via 2 checks

Senior management should be assigned

Compliance Policy

DECLARED via 1 check

Management Review of Internal Audit

Control **SDC 154**

Entity has set up mechanisms to assign and manage asset ownership responsibilities and establish a common understanding of asset protection requirements.

MONITORED via 1 check

Infrastructure operations person should be assigned

Control **SDC 396**

Entity appoints a People Operations Officer to develop and drive all personnel-related security strategies.

MONITORED via 2 checks

People operations person should be assigned

HR Security Policy

Control **SDC 397**

Entity appoints a Compliance Program Manager who is delegated the responsibility of planning and implementing the internal control environment.

MONITORED via 3 checks

Compliance program manager should be assigned

Compliance Procedure

Compliance Policy

164.308(a)(3)(ii)(A)

Authorization and/or supervision: Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

INTERNAL CONTROLS AND CHECKS

Control **SDC 33**

Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.

MONITORED via 2 checks

Access Control Procedure
Access Control Policy

Control **SDC 34**

Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.

MONITORED via 6 checks

User access to critical system should be validated by roles
Role based access should be setup
HR Security Procedure
Access Control Procedure
HR Security Policy
Access Control Policy

Control **SDC 35**

Entity ensures logical access that is no longer required in the event of termination is made inaccessible in a timely manner.

MONITORED via 4 checks

HR Security Procedure
Access Control Procedure
HR Security Policy
Access Control Policy

Control **SDC 37**

Entity ensures that access to the production databases is restricted to only those individuals who require such access to perform their job functions.

MONITORED via 5 checks

Access to critical systems should be reviewed

Policies should be attached to groups and should not be attached to users
Users of critical system should be identified
Access Control Procedure
Access Control Policy

Control **SDC 38**

Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.

MONITORED via 1 check

Public access for infra assets should be restricted

Control **SDC 39**

Entity requires that all staff members with access to any critical system be protected with a secure login mechanism such as Multifactor-authentication.

MONITORED via 3 checks

Critical systems should be protected with a secure login mechanism
Access Control Procedure
Access Control Policy

DECLARED via 1 check

Access should be protected with secure login mechanism

Control **SDC 42**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

MONITORED via 4 checks

Access to critical systems should be reviewed
Users of critical system should be identified
Access Control Procedure
Access Control Policy

Control **SDC 43**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such

access to perform their job functions.

MONITORED via 4 checks

Access to critical systems should be reviewed
Users of critical system should be identified
Access Control Procedure
Access Control Policy

164.308(a)(3)(ii)(B)

Workforce clearance procedure: Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

INTERNAL CONTROLS AND CHECKS

Control **SDC 33**

Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.

MONITORED via 2 checks

Access Control Procedure
Access Control Policy

Control **SDC 34**

Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.

MONITORED via 6 checks

User access to critical system should be validated by roles
Role based access should be setup
HR Security Procedure
Access Control Procedure
HR Security Policy
Access Control Policy

Control **SDC 35**

Entity ensures logical access that is no longer required in the event of termination is made inaccessible in a timely manner.

MONITORED via 4 checks

HR Security Procedure
Access Control Procedure
HR Security Policy
Access Control Policy

Control **SDC 37**

Entity ensures that access to the production databases is restricted to only those individuals who require such access to perform their job functions.

MONITORED via 5 checks

Access to critical systems should be reviewed
Policies should be attached to groups and should not be attached to users
Users of critical system should be identified
Access Control Procedure
Access Control Policy

Control **SDC 38**

Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.

MONITORED via 1 check

Public access for infra assets should be restricted

Control **SDC 39**

Entity requires that all staff members with access to any critical system be protected with a secure login mechanism such as Multifactor-authentication.

MONITORED via 3 checks

Critical systems should be protected with a secure login mechanism
Access Control Procedure
Access Control Policy

DECLARED via 1 check

Access should be protected with secure login mechanism

Control **SDC 42**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

MONITORED via 4 checks

Access to critical systems should be reviewed
Users of critical system should be identified
Access Control Procedure
Access Control Policy

Control **SDC 43**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

MONITORED via 4 checks

Access to critical systems should be reviewed
Users of critical system should be identified
Access Control Procedure
Access Control Policy

164.308(a)(3)(ii)(C)

Termination procedures: Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) [the Workforce Clearance Procedure] of this section.

INTERNAL CONTROLS AND CHECKS

Control **SDC 35**

Entity ensures logical access that is no longer required in the event of termination is made inaccessible in a timely manner.

MONITORED via 4 checks

HR Security Procedure
Access Control Procedure
HR Security Policy
Access Control Policy

Control SDC 33

Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.

MONITORED via 2 checks

Access Control Procedure
Access Control Policy

164.308(a)(4)(i)

Information access management: Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of the Privacy Rule. Policies and procedures should include: Isolating Health Care Clearinghouse Functions, Access Authorization and Access Establishment and Modification.

INTERNAL CONTROLS AND CHECKS

Control SDC 33

Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.

MONITORED via 2 checks

Access Control Procedure
Access Control Policy

Control SDC 34

Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.

MONITORED via 6 checks

User access to critical system should be validated by roles
Role based access should be setup
HR Security Procedure
Access Control Procedure
HR Security Policy

Access Control Policy

Control **SDC 35**

Entity ensures logical access that is no longer required in the event of termination is made inaccessible in a timely manner.

MONITORED via 4 checks

HR Security Procedure
Access Control Procedure
HR Security Policy
Access Control Policy

Control **SDC 37**

Entity ensures that access to the production databases is restricted to only those individuals who require such access to perform their job functions.

MONITORED via 5 checks

Access to critical systems should be reviewed
Policies should be attached to groups and should not be attached to users
Users of critical system should be identified
Access Control Procedure
Access Control Policy

Control **SDC 38**

Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.

MONITORED via 1 check

Public access for infra assets should be restricted

Control **SDC 39**

Entity requires that all staff members with access to any critical system be protected with a secure login mechanism such as Multifactor-authentication.

MONITORED via 3 checks

Critical systems should be protected with a secure login mechanism
Access Control Procedure
Access Control Policy

DECLARED via 1 check

Access should be protected with secure login mechanism

Control **SDC 42**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

MONITORED via 4 checks

Access to critical systems should be reviewed
Users of critical system should be identified
Access Control Procedure
Access Control Policy

Control **SDC 43**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

MONITORED via 4 checks

Access to critical systems should be reviewed
Users of critical system should be identified
Access Control Procedure
Access Control Policy

164.308(a)(4)(ii)(B)

Access authorization: Implement policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, process, or other mechanism.

INTERNAL CONTROLS AND CHECKS

Control **SDC 33**

Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.

MONITORED via 2 checks

Access Control Procedure
Access Control Policy

Control SDC 34

Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.

MONITORED via 6 checks

User access to critical system should be validated by roles
Role based access should be setup
HR Security Procedure
Access Control Procedure
HR Security Policy
Access Control Policy

Control SDC 35

Entity ensures logical access that is no longer required in the event of termination is made inaccessible in a timely manner.

MONITORED via 4 checks

HR Security Procedure
Access Control Procedure
HR Security Policy
Access Control Policy

Control SDC 38

Entity ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.

MONITORED via 1 check

Public access for infra assets should be restricted

Control SDC 37

Entity ensures that access to the production databases is restricted to only those individuals who require such access to perform their job functions.

MONITORED via 5 checks

Access to critical systems should be reviewed
Policies should be attached to groups and should not be attached to users
Users of critical system should be identified
Access Control Procedure
Access Control Policy

Control **SDC 39**

Entity requires that all staff members with access to any critical system be protected with a secure login mechanism such as Multifactor-authentication.

MONITORED via 3 checks

Critical systems should be protected with a secure login mechanism
Access Control Procedure
Access Control Policy

DECLARED via 1 check

Access should be protected with secure login mechanism

Control **SDC 42**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

MONITORED via 4 checks

Access to critical systems should be reviewed
Users of critical system should be identified
Access Control Procedure
Access Control Policy

Control **SDC 43**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

MONITORED via 4 checks

Access to critical systems should be reviewed
Users of critical system should be identified
Access Control Procedure
Access Control Policy

164.308(a)(4)(ii)(C)

Access establishment and modification: Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

INTERNAL CONTROLS AND CHECKS

Control **SDC 33**

Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.

MONITORED via 2 checks

Access Control Procedure
Access Control Policy

Control **SDC 34**

Entity ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.

MONITORED via 6 checks

User access to critical system should be validated by roles
Role based access should be setup
HR Security Procedure
Access Control Procedure
HR Security Policy
Access Control Policy

Control **SDC 42**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

MONITORED via 4 checks

Access to critical systems should be reviewed
Users of critical system should be identified
Access Control Procedure
Access Control Policy

Control **SDC 43**

Entity's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such access to perform their job functions.

MONITORED via 4 checks

Access to critical systems should be reviewed
Users of critical system should be identified
Access Control Procedure
Access Control Policy

164.308(a)(5)(i)

Security awareness and training: Implement a security awareness and training program for all members of the workforce (including management). Component of the Security Awareness and Training program should include Security Reminders, Protection Malicious Software, Log-in Monitoring and Password Management.

INTERNAL CONTROLS AND CHECKS

Control **SDC 1**

Entity has a documented policy to define behavioral standards and acceptable business conduct.

MONITORED via 1 check

Code of Business Conduct Policy

Control **SDC 7**

Entity provides information security and privacy training to staff that is relevant to their job function.

MONITORED via 2 checks

Security training provider should be configured
HR Security Policy

Control **SDC 387**

Entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.

MONITORED via 3 checks

Infosec training should be completed by onboarded staff
HR Security Procedure
HR Security Policy

Control SDC 388

Entity documents, monitors, and retains individual training activities and records.

MONITORED via 2 checks

Infosec training should be completed by onboarded staff
Staff should periodically complete security training

164.308(a)(5)(ii)(A)

Security reminders: Periodic security updates.

INTERNAL CONTROLS AND CHECKS

Control SDC 46

Entity has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.

MONITORED via 5 checks

Staff devices should have OS updated
Endpoint Security Policy
Asset Management Policy
Physical and Environmental Security Procedure
Asset Management Procedure

Control SDC 110

To help determine that only authorized changes are deployed, Entity's key personnel are notified when changes are deployed to the production environment

DECLARED via 1 check

Deployment Notifications

164.308(a)(5)(ii)(B)

Protection from malicious software: Procedures for guarding against, detecting, and reporting malicious software.

INTERNAL CONTROLS AND CHECKS

Control **SDC 44**

Where applicable, Entity ensures that endpoints with access to critical servers or data must be protected by malware-protection software.

MONITORED via 5 checks

Staff devices should have antivirus running
Endpoint Security Policy
Asset Management Policy
Physical and Environmental Security Procedure
Asset Management Procedure

Control **SDC 104**

Entity has documented policies and procedures for endpoint security and related controls.

MONITORED via 3 checks

Endpoint Security Policy
Asset Management Policy
Asset Management Procedure

164.308(a)(5)(ii)(C)

Log-in monitoring: Procedures for monitoring log-in attempts and reporting discrepancies.

INTERNAL CONTROLS AND CHECKS

Control **SDC 394**

Entity's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.

MONITORED via 3 checks

Audit logs should exist
Operation Security Policy
Operations Security Procedure

Control **SDC 50**

Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the Entity's cloud provider.

MONITORED via 4 checks

Infrastructure provider should be configured
Asset Management Policy
Network Security Procedure
Asset Management Procedure

DECLARED via 1 check

Deny by default firewall ruleset should be set up on all production hosts

164.308(a)(5)(ii)(D)

Password management: Procedures for creating, changing, and safeguarding passwords.

INTERNAL CONTROLS AND CHECKS

Control **SDC 33**

Entity has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.

MONITORED via 2 checks

Access Control Procedure
Access Control Policy

Control **SDC 135**

Entity has documented guidelines to manage passwords and secure login mechanisms and makes them available to all staff members on the company employee portal.

MONITORED via 3 checks

Access Control Procedure
Acceptable Usage Policy
Access Control Policy

164.308(a)(6)(i)

Security incident procedures: Implement policies and procedures to address security incidents. Policies and procedures should include response reporting.

INTERNAL CONTROLS AND CHECKS

Control **SDC 15**

Entity has provided information to employees, via various Information Security Policies/procedures, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the entity in the event there are problems.

MONITORED via 1 check

Information Security Policy

Control **SDC 16**

Entity has provided information to customers on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the Entity in the event there are problems.

MONITORED via 1 check

Customer support page (Contact Us) should be available

Control **SDC 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.

MONITORED via 2 checks

Incident Management Procedure
Incident Management Policy

Control **SDC 54**

Entity maintains a record of information security incidents, its investigation, and the response plan that was executed in accordance with the policy and procedure defined to report and manage incidents.

MONITORED via 1 check

Incidents should be investigated based on severity

Control **SDC 61**

Entity's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats

MONITORED via 1 check

Threat detection system should be enabled

Control **SDC 62**

Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.

MONITORED via 4 checks

Health of production infrastructure should be monitored
Errors on production infrastructure should be monitored
Operation Security Policy
Operations Security Procedure

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.

INTERNAL CONTROLS AND CHECKS

Control **SDC 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.

MONITORED via 2 checks

Incident Management Procedure
Incident Management Policy

Control SDC 393

Entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.

MONITORED via 2 checks

Business Continuity Plan
Business Continuity & Disaster Recovery Policy

Control SDC 392

Entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident

MONITORED via 2 checks

Business Continuity Plan
Business Continuity & Disaster Recovery Policy

164.308(a)(7)(ii)(A)

Data backup plan: Establish and implement procedures to create and maintain retrievable exact copies of ePHI.

INTERNAL CONTROLS AND CHECKS

Control SDC 58

Entity has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal

MONITORED via 2 checks

Operation Security Policy

Operations Security Procedure

Control **SDC 59**

Entity backs up relevant user and system data regularly to meet recovery time and recovery point objectives and verifies the integrity of these backups.

MONITORED via 5 checks

Backup should be enabled on production database
Versioning should be enabled for storage assets
Operation Security Policy
Business Continuity Plan
Operations Security Procedure

Control **SDC 60**

Entity tests backup information periodically to verify media reliability and information integrity.

DECLARED via 1 check

Data backup restoration

164.308(a)(7)(ii)(B)

Disaster recovery plan: Establish (and implement as needed) procedures to restore any loss of data.

INTERNAL CONTROLS AND CHECKS

Control **SDC 60**

Entity tests backup information periodically to verify media reliability and information integrity.

DECLARED via 1 check

Data backup restoration

Control **SDC 97**

Entity has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.

DECLARED via 1 check

Disaster recovery

Control SDC 392

Entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident

MONITORED via 2 checks

Business Continuity Plan
Business Continuity & Disaster Recovery Policy

Control SDC 393

Entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.

MONITORED via 2 checks

Business Continuity Plan
Business Continuity & Disaster Recovery Policy

164.308(a)(7)(ii)(C)

Emergency Mode Operation Plan: Establish and implement procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.

INTERNAL CONTROLS AND CHECKS

Control SDC 53

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.

MONITORED via 2 checks

Incident Management Procedure
Incident Management Policy

Control SDC 112

Entity has documented guidelines on notifying customers and other stakeholders in case of a breach.

MONITORED via 3 checks

Data Breach Notification Policy
PHI Data breach Notification Procedure
Personal Data Breach Notification Procedure

Control **SDC 113**

Entity conducts risk assessment of suspected data breaches and any significant data breaches are notified to all affected parties without unreasonable delay.

MONITORED via 3 checks

Incidents should be investigated based on severity
Incident Management Procedure
Incident Management Policy

164.308(a)(7)(ii)(D)

Testing and revision procedures: Implement procedures for periodic testing and revision of contingency plans.

INTERNAL CONTROLS AND CHECKS

Control **SDC 393**

Entity has documented policies and procedures that establish guidelines for continuing business operations and facilitate the application of contingency planning controls.

MONITORED via 2 checks

Business Continuity Plan
Business Continuity & Disaster Recovery Policy

Control **SDC 392**

Entity has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident

MONITORED via 2 checks

Business Continuity Plan

Business Continuity & Disaster Recovery Policy

164.308(a)(7)(ii)(E)

Applications and data criticality analysis: Assess the relative criticality of specific applications and data in support of another contingency plan component.

INTERNAL CONTROLS AND CHECKS

Control **SDC 18**

Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.

MONITORED via 2 checks

Risk assessment should be conducted periodically
Risk Assessment & Management Policy

Control **SDC 19**

Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.

MONITORED via 1 check

Risk assessment should be conducted periodically

Control **SDC 20**

Entity considers the potential for fraud when assessing risks. This is an entry in the risk matrix.

MONITORED via 1 check

Risk assessment should be conducted periodically

Control **SDC 67**

Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the Entity's

service commitments and system requirements

MONITORED via 1 check

Risk Assessment & Management Policy

164.308(a)(8)

Evaluation: Perform a periodic technical and nontechnical evaluation based initially upon the standards implemented under this rule and subsequently, in response to environmental or operations changes affecting the security of ePHI, that establishes the extent to which an entity’s security policies and procedures meet the requirement.

INTERNAL CONTROLS AND CHECKS

Control **SDC 18**

Entity performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.

MONITORED via 2 checks

Risk assessment should be conducted periodically

Risk Assessment & Management Policy

Control **SDC 19**

Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.

MONITORED via 1 check

Risk assessment should be conducted periodically

Control **SDC 20**

Entity considers the potential for fraud when assessing risks. This is an entry in the risk matrix.

MONITORED via 1 check

Risk assessment should be conducted periodically

Control **SDC 27**

Entity's Senior Management reviews and approves the "Risk Assessment Report" annually.

MONITORED via 2 checks

Risk assessment should be reviewed by senior management
Risk Assessment & Management Policy

Control **SDC 67**

Entity has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the Entity's service commitments and system requirements

MONITORED via 1 check

Risk Assessment & Management Policy

Control **SDC 63**

Entity identifies vulnerabilities on the company platform through an annual penetration testing exercise conducted by a qualified third-party service provider.

MONITORED via 1 check

VAPT exercise should be conducted annually

Control **SDC 55**

Entity identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.

MONITORED via 2 checks

Vulnerability should be closed in SLA
Vulnerability scanner should be enabled

Control **SDC 56**

Entity tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.

MONITORED via 1 check

Vulnerability should be closed in SLA

164.308(b)(1)

Business associate contracts and other arrangements: A covered entity, in accordance with 164.306 The Security Standards: General Rules], may permit a business associate to create, receive, maintain, or transmit ePHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with 164.314 [the Organization Requirements] that the business associate will appropriately safeguard the information.

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

MONITORED via 2 checks

Vendor risk assessment should be conducted periodically
Vendor Management Policy

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

MONITORED via 3 checks

Vendor risk assessment should be reviewed by senior management
Vendor Management Policy
Vendor Management Procedure

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

MONITORED via 1 check

Vendor Management Policy

Control SDC 77

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

MONITORED via 2 checks

Vendor risk assessment should be conducted periodically
Vendor Management Policy

164.308(b)(2)

A business associate may permit a business that is a subcontractor to create, receive, maintain, or transmit ePHI on its behalf only if the business associate obtains satisfactory assurances, in accordance with §164.314(a), that the subcontractor will appropriately safeguard the information.

INTERNAL CONTROLS AND CHECKS

Control SDC 21

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

MONITORED via 2 checks

Vendor risk assessment should be conducted periodically
Vendor Management Policy

Control SDC 29

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

MONITORED via 3 checks

Vendor risk assessment should be reviewed by senior management
Vendor Management Policy
Vendor Management Procedure

Control SDC 68

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

MONITORED via 1 check

Vendor Management Policy

164.314

Organizational requirements

164.314(b)(2)(i)

Safeguards: Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits on behalf of the group health plan

INTERNAL CONTROLS AND CHECKS

Control **SDC 64**

Entity has documented policies and procedures to manage changes to its operating environment.

MONITORED via 4 checks

SDLC Procedure
Operation Security Policy
Operations Security Procedure
System Acquisition and Development Lifecycle Policy

Control **SDC 65**

Entity has procedures to govern changes to its operating environment.

MONITORED via 5 checks

Change management repos should be classified
Change management source should be configured
SDLC Procedure
Operation Security Policy
Operations Security Procedure

Control **SDC 66**

Entity has established procedures for approval when implementing changes to the operating environment.

MONITORED via 5 checks

Changes to production code should be reviewed by peers
Change requests should be reviewed by peers
SDLC Procedure
Operation Security Policy
Operations Security Procedure

Control **SDC 119**

Entity has documented guidelines to manage communications protections and network security of critical systems.

MONITORED via 2 checks

Communications & Network Security Policy
Network Security Procedure

Control **SDC 432**

Entity outlines and documents cybersecurity responsibilities for all personnel.

MONITORED via 1 check

Organization of Information Security Policy

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

MONITORED via 2 checks

Vendor risk assessment should be conducted periodically
Vendor Management Policy

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

MONITORED via 3 checks

Vendor risk assessment should be reviewed by senior management
Vendor Management Policy
Vendor Management Procedure

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

MONITORED via 2 checks

Vendor risk assessment should be conducted periodically
Vendor Management Policy

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

MONITORED via 1 check

Vendor Management Policy

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

MONITORED via 2 checks

Vendor risk assessment should be conducted periodically
Vendor Management Policy

Control **SDC 97**

Entity has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.

DECLARED via 1 check

Disaster recovery

Control **SDC 98**

Entity maintains a list of all contractual obligations based on customer contracts.

DECLARED via 1 check

Management review of contractual obligations

Control **SDC 100**

Entity ensures that customer data used in non-Production environments requires the same level of protection as the production environment.

MONITORED via 3 checks

Critical Infrastructure assets should be identified
Asset Management Policy
Asset Management Procedure

Control **SDC 143**

Entity has a documented Privacy Policy which meets all the regulatory requirements and is published on the company's website.

MONITORED via 1 check

Privacy policy should be available on the product website

Control **SDC 144**

Entity includes Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.

DECLARED via 1 check

Review of the privacy policy

Control **SDC 141**

Entity requires that all critical endpoints are encrypted to protect them from unauthorized access.

MONITORED via 7 checks

Staff devices should have disk encryption enabled
Staff devices health should be monitored regularly
Endpoint Security Policy
Asset Management Policy
Physical and Environmental Security Procedure
Asset Management Procedure
Acceptable Usage Policy

Control **SDC 59**

Entity backs up relevant user and system data regularly to meet recovery time and recovery point objectives and verifies the integrity of these backups.

MONITORED via 5 checks

Backup should be enabled on production database
Versioning should be enabled for storage assets
Operation Security Policy
Business Continuity Plan
Operations Security Procedure

Control **SDC 62**

Entity has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.

MONITORED via 4 checks

Health of production infrastructure should be monitored
Errors on production infrastructure should be monitored
Operation Security Policy
Operations Security Procedure

Control **SDC 69**

Entity has a documented Information Security Policy that governs the confidentiality, integrity, and availability of information systems

MONITORED via 1 check

Information Security Policy

Control **SDC 74**

Entity ensures appropriate procedures are in place to ensure compliance with regulatory requirements related to transfer of personal data outside of the region from which it is collected

MONITORED via 2 checks

Vendor risk assessment should be conducted periodically
Vendor Management Policy

Control **SDC 114**

Entity appoints a Privacy Officer to assess and facilitate the entity's compliance with relevant regulatory requirements.

MONITORED via 1 check

Privacy officer should be assigned

Control **SDC 387**

Entity has established procedures for new staff to complete security and privacy literacy training as a part of their onboarding.

MONITORED via 3 checks

Infosec training should be completed by onboarded staff
HR Security Procedure
HR Security Policy

Control **SDC 388**

Entity documents, monitors, and retains individual training activities and records.

MONITORED via 2 checks

Infosec training should be completed by onboarded staff
Staff should periodically complete security training

Control **SDC 390**

Entity develops, documents, and maintains an inventory of organizational endpoint systems, including all necessary information to achieve accountability.

MONITORED via 3 checks

Staff devices health should be monitored regularly
Endpoint Security Policy
Asset Management Procedure

Control **SDC 389**

Entity periodically updates and reviews the inventory of systems as a part of installations, removals, and system updates.

MONITORED via 2 checks

Asset Management Policy

Asset Management Procedure

DECLARED via 1 check

Internal Audit

Control **SDC 9**

Entity requires that all employees in client serving, IT, Engineering, and Information Security roles are periodically evaluated regarding their job responsibilities.

MONITORED via 2 checks

HR Security Procedure

HR Security Policy

DECLARED via 1 check

Staff Performance Evaluations

Control **SDC 11**

Entity systems generate information that is reviewed and evaluated to determine impacts on the functioning of internal controls.

MONITORED via 3 checks

Health of production infrastructure should be monitored

Asset Management Policy

Asset Management Procedure

Control **SDC 19**

Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.

MONITORED via 1 check

Risk assessment should be conducted periodically

Control **SDC 23**

Entity uses Sprinto, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.

DECLARED via 1 check

Internal Audit

Control **SDC 49**

Entity has set up cryptographic mechanisms to encrypt all production database[s] that store customer data at rest.

MONITORED via 4 checks

Data at rest should be encrypted
Encryption Policy
Asset Management Policy
Asset Management Procedure

Control **SDC 52**

Entity develops, documents, and maintains an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.

MONITORED via 1 check

Critical Infrastructure assets should be identified

164.314(a)(1)

Business associate contracts or other arrangements: A covered entity is not in compliance with the standards in § 164.502(e) if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate’s obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful - (A)Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary.”

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

MONITORED via 2 checks

Vendor risk assessment should be conducted periodically
Vendor Management Policy

Control SDC 29

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

MONITORED via 3 checks

Vendor risk assessment should be reviewed by senior management
Vendor Management Policy
Vendor Management Procedure

Control SDC 30

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

MONITORED via 2 checks

Vendor risk assessment should be conducted periodically
Vendor Management Policy

Control SDC 68

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

MONITORED via 1 check

Vendor Management Policy

Control SDC 77

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

MONITORED via 2 checks

Vendor risk assessment should be conducted periodically
Vendor Management Policy

164.314(a)(2)(i)

Business Associate Contracts: A business associate contract must provide that the business associate will: “Implement safeguards that protect the confidentiality, integrity, and availability of the electronic protected health...; Report to the covered entity any security incident of which it becomes aware; Authorize termination of the contract, if the covered entity determines that the business associate has violated a material term of the contract.”

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

MONITORED via 2 checks

Vendor risk assessment should be conducted periodically
Vendor Management Policy

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

MONITORED via 3 checks

Vendor risk assessment should be reviewed by senior management
Vendor Management Policy
Vendor Management Procedure

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

MONITORED via 2 checks

Vendor risk assessment should be conducted periodically
Vendor Management Policy

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

MONITORED via 2 checks

Vendor risk assessment should be conducted periodically

Vendor Management Policy

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

MONITORED via 1 check

Vendor Management Policy

Control **SDC 75**

Entity maintains an inventory of categories of personal information collected along with its usage, sources and specific purposes for collection as per regulatory requirements ("Record of Processing Activities") and reviews it on an annual basis

DECLARED via 1 check

Records of Processing Activities (ROPA) & Data flow map

Control **SDC 76**

Entity ensures regulatory requirements regarding user consent are met prior to processing personal data

DECLARED via 1 check

Data consent using cookie banner

Control **SDC 79**

Entity conducts Data Protection Impact Assessments periodically in order to assess the regulatory risks associated with the processing of personal data

MONITORED via 1 check

Risk assessment should be conducted periodically

Control **SDC 80**

Entity ensures that Subject Access Requests are being honored in accordance with the Privacy Policy

DECLARED via 1 check

Data Subject Access Requests (SARs) Report

Control SDC 95

A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.

MONITORED via 2 checks

Endpoint Security Policy
Acceptable Usage Policy

164.314(a)(2)(iii)

Business associate contracts with subcontractors: The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by §164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.

INTERNAL CONTROLS AND CHECKS

Control SDC 21

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

MONITORED via 2 checks

Vendor risk assessment should be conducted periodically
Vendor Management Policy

Control SDC 29

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

MONITORED via 3 checks

Vendor risk assessment should be reviewed by senior management
Vendor Management Policy

Vendor Management Procedure

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

MONITORED via 2 checks

Vendor risk assessment should be conducted periodically
Vendor Management Policy

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

MONITORED via 1 check

Vendor Management Policy

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

MONITORED via 2 checks

Vendor risk assessment should be conducted periodically
Vendor Management Policy

164.314(b)(2)(iii)

Agreement: Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information

INTERNAL CONTROLS AND CHECKS

Control **SDC 21**

Entity performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.

MONITORED via 2 checks

Vendor risk assessment should be conducted periodically
Vendor Management Policy

Control **SDC 29**

Entity's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.

MONITORED via 3 checks

Vendor risk assessment should be reviewed by senior management
Vendor Management Policy
Vendor Management Procedure

Control **SDC 30**

Entity reviews and evaluates all subservice organizations periodically, to ensure commitments to Entity's customers can be met.

MONITORED via 2 checks

Vendor risk assessment should be conducted periodically
Vendor Management Policy

Control **SDC 68**

Entity has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors

MONITORED via 1 check

Vendor Management Policy

Control **SDC 77**

Entity ensures that appropriate remediation measures are in place when personal data is shared with vendors as a part of its processing activities

MONITORED via 2 checks

Vendor risk assessment should be conducted periodically
Vendor Management Policy

164.314(b)(2)(iv)

Reporting: Report to the group health plan any security incident of which it becomes aware

INTERNAL CONTROLS AND CHECKS

Control **SDC 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.

MONITORED via 2 checks

Incident Management Procedure
Incident Management Policy

Control **SDC 112**

Entity has documented guidelines on notifying customers and other stakeholders in case of a breach.

MONITORED via 3 checks

Data Breach Notification Policy
PHI Data breach Notification Procedure
Personal Data Breach Notification Procedure

Control **SDC 113**

Entity conducts risk assessment of suspected data breaches and any significant data breaches are notified to all affected parties without unreasonable delay.

MONITORED via 3 checks

Incidents should be investigated based on severity
Incident Management Procedure
Incident Management Policy

About Sprinto

Sprinto is a modern platform for continuous compliance monitoring. It automates the detection, remediation, and management of security risks, ensuring ongoing compliance with leading security and privacy standards.