HIPAA Readiness report for Product Fruits s.r.o.

Generated on 03 November 2023

Report summary

This report provides a summary of Product Fruits s.r.o.'s readiness posture for HIPAA certification as of 3rd November 2023. Sprinto continuously monitors the security and readiness posture of Product Fruits s.r.o. to ensure you have a transparent view into how they have setup Sprinto to meet industry standards. 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.

Legend

✓ Check is healthy

◷ Check is work in progress

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 **SPR 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

Tested via 1 check

Information security policy should be defined	✓

Control **SPR 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents. This is available to all staff members via the company employee portal.

Tested via 2 checks

Incident management policy should be defined	✓
Incident management procedure should be defined	✓

Control **SPR 112**

Entity has documented guidelines on notifying customers and other stakeholders in case of a breach and makes it available for all staff on the company employee portal

Tested via 1 check

Phi breach notification policy should be defined	✓

Control **SPR 100**

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

Tested via 1 check

Critical Infrastructure assets should be identified	✓

Control **SPR 104**

Entity has documented guidelines for endpoint security and makes it available for all staff on the company employee portal

Tested via 3 checks

Asset management policy should be defined	✓
Asset management procedure should be defined	✓
Endpoint security policy should be defined	✓

Control **SPR 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

Tested via 1 check

Access to critical systems should be reviewed	✓

Control **SPR 433**

Entity has an established a policy which provides guidance on integrating privacy principles into the design process that help in complying with privacy regulations and makes it available to all staff members on the company employee portal

Tested via 1 check

Privacy by design policy should be defined ✓

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 **SPR 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

Tested via 1 check

Risk assessment should be conducted periodically ✓

Control **SPR 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 Entity's service commitments and system requirements

Tested via 1 check

Risk assessment & management policy should be defined ✓

Control **SPR 391**

Entity has a documented policy to establish guidelines on managing technical vulnerabilities and makes it available for all staff on the company employee portal

Tested via 3 checks

Operation security policy should be defined	✓
Operations security procedure should be defined	✓
Vulnerability management policy should be defined	✓

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 **SPR 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

Tested via 1 check

Risk assessment should be conducted periodically	✓

Control **SPR 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 Entity's service commitments and system requirements

Tested via 1 check

Risk assessment & management policy should be defined ✓

Control **SPR 5**

Entity ensures that new hires go through a background check as part of their onboarding process

Tested via 1 check

Background checks should be conducted for new employees ✓

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 **SPR 6**

Entity requires that new staff members review and acknowledge relevant company policies, including the code of business conduct, as part of their onboarding. This ensures they understand their responsibilities and are willing to comply with them

Tested via 1 check

Policies should be acknowledged by new staff ✓

Control **SPR 12**

Entity requires that all staff members review and acknowledge company policies annually

Tested via 1 check

Staff should periodically acknowledge policies ✓

Control **SPR 13**

Entity makes all policies and procedures available to all staff members via the company employee portal

Tested via 0 checks

Control **SPR 31**

Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.

Tested 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 **SPR 33**

Entity has developed a policy 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

Tested via 2 checks

Access control policy should be defined	✓
Access control procedure should be defined	✓

Control **SPR 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents. This is available to all staff members via the company employee portal.

Tested via 2 checks

Incident management policy should be defined	✓
Incident management procedure should be defined	✓

Control **SPR 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

Tested 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 **SPR 22**

Entity's Senior Management assigns the role of Information Security Officer who is delegated the responsibility of planning, assessing, implementing and reviewing the internal control environment.

Tested via 1 check

Information security officer should be assigned	✓

Control **SPR 25**

Entity's Senior Management reviews and approves the state of the Information Security program annually

Tested via 2 checks

Management Review of Internal Audit	✓
Senior management should be assigned	✓

Control **SPR 154**

Entity appoints an owner of Infrastructure operations, who is responsible for all assets in the inventory

Tested via 1 check

Infrastructure operations person should be assigned	✓

Control **SPR 396**

Entity appoints a People Operations Officer to develop and drive forward all HR security-related strategies across the company

Tested via 1 check

People operations person should be assigned	✓

Control **SPR 397**

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

Tested via 1 check

Compliance program manager should be assigned	✓

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 **SPR 33**

Entity has developed a policy 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

Tested via 2 checks

Access control policy should be defined	✓
Access control procedure should be defined	✓

Control **SPR 34**

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

Tested via 2 checks

User access to critical system should be validated by roles	✓
Role based access should be setup	✓

Control **SPR 35**

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

Tested via 0 checks

Control **SPR 37**

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

Tested via 3 checks

User Access Reviews for Critical Systems	✓
Access to critical systems should be reviewed	✓
Users of critical system should be identified	✓

Control **SPR 38**

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

Tested via 1 check

Public access for infra assets should be restricted	✓

Control **SPR 39**

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

Tested via 4 checks

MFA Enforced by System Configuration	✓
Office365 User MFA Status	✓
Password Complexity Enforced by System Configuration	✓
Users should have MFA enabled for login	✓

Control **SPR 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

Tested via 3 checks

User Access Reviews for Critical Systems	✓
Access to critical systems should be reviewed	✓
Users of critical system should be identified	✓

Control **SPR 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

Tested via 3 checks

User Access Reviews for Critical Systems	✓
Access to critical systems should be reviewed	✓
Users of critical system should be identified	✓

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 **SPR 33**

Entity has developed a policy 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

Tested via 2 checks

Access control policy should be defined	✓
Access control procedure should be defined	✓

Control **SPR 34**

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

Tested via 2 checks

User access to critical system should be validated by roles	✓
Role based access should be setup	✓

Control **SPR 35**

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

Tested via 0 checks

Control **SPR 37**

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

Tested via 3 checks

User Access Reviews for Critical Systems	✓
Access to critical systems should be reviewed	✓

Users of critical system should be identified ✓

Control **SPR 38**

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

Tested via 1 check

Public access for infra assets should be restricted	✓

Control **SPR 39**

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

Tested via 4 checks

MFA Enforced by System Configuration	✓
Office365 User MFA Status	✓
Password Complexity Enforced by System Configuration	✓
Users should have MFA enabled for login	✓

Control **SPR 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

Tested via 3 checks

User Access Reviews for Critical Systems	✓
Access to critical systems should be reviewed	✓

Users of critical system should be identified ✓

Control **SPR 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

Tested via 3 checks

User Access Reviews for Critical Systems ✓

Access to critical systems should be reviewed ✓

Users of critical system should be identified ✓

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 **SPR 33**

Entity has developed a policy 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

Tested via 2 checks

Access control policy should be defined ✓

Access control procedure should be defined ✓

Control **SPR 34**

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

Tested via 2 checks

User access to critical system should be validated by roles	✓
Role based access should be setup	✓

Control **SPR 35**

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

Tested via 0 checks

Control **SPR 37**

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

Tested via 3 checks

User Access Reviews for Critical Systems	✓
Access to critical systems should be reviewed	✓
Users of critical system should be identified	✓

Control **SPR 38**

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

Tested via 1 check

Public access for infra assets should be restricted	✓

Control **SPR 39**

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

Tested via 4 checks

MFA Enforced by System Configuration	✓
Office365 User MFA Status	✓
Password Complexity Enforced by System Configuration	✓
Users should have MFA enabled for login	✓

Control **SPR 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

Tested via 3 checks

User Access Reviews for Critical Systems	✓
Access to critical systems should be reviewed	✓
Users of critical system should be identified	✓

Control **SPR 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

Tested via 3 checks

User Access Reviews for Critical Systems	✓

Access to critical systems should be reviewed	✓
Users of critical system should be identified	✓

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 **SPR 35**

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

Tested via 0 checks

Control **SPR 33**

Entity has developed a policy 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

Tested via 2 checks

Access control policy should be defined	✓
Access control procedure should be defined	✓

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 **SPR 33**

Entity has developed a policy 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

Tested via 2 checks

Access control policy should be defined	✓
Access control procedure should be defined	✓

Control **SPR 34**

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

Tested via 2 checks

User access to critical system should be validated by roles	✓
Role based access should be setup	✓

Control **SPR 35**

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

Tested via 0 checks

Control **SPR 37**

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

Tested via 3 checks

User Access Reviews for Critical Systems	✓
Access to critical systems should be reviewed	✓
Users of critical system should be identified	✓

Control **SPR 38**

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

Tested via 1 check

Public access for infra assets should be restricted	✓

Control **SPR 39**

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

Tested via 4 checks

MFA Enforced by System Configuration	✓
Office365 User MFA Status	✓
Password Complexity Enforced by System Configuration	✓
Users should have MFA enabled for login	✓

Control **SPR 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

Tested via 3 checks

User Access Reviews for Critical Systems	✓
Access to critical systems should be reviewed	✓
Users of critical system should be identified	✓

Control **SPR 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

Tested via 3 checks

User Access Reviews for Critical Systems	✓
Access to critical systems should be reviewed	✓
Users of critical system should be identified	✓

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 **SPR 33**

Entity has developed a policy 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

Tested via 2 checks

Access control policy should be defined	✓
Access control procedure should be defined	✓

Control **SPR 34**

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

Tested via 2 checks

User access to critical system should be validated by roles	✓
Role based access should be setup	✓

Control **SPR 35**

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

Tested via 0 checks

Control **SPR 38**

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

Tested via 1 check

Public access for infra assets should be restricted	✓

Control **SPR 37**

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

Tested via 3 checks

User Access Reviews for Critical Systems	✓
Access to critical systems should be reviewed	✓
Users of critical system should be identified	✓

Control **SPR 39**

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

Tested via 4 checks

MFA Enforced by System Configuration	✓
Office365 User MFA Status	✓
Password Complexity Enforced by System Configuration	✓
Users should have MFA enabled for login	✓

Control **SPR 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

Tested via 3 checks

User Access Reviews for Critical Systems	✓
Access to critical systems should be reviewed	✓
Users of critical system should be identified	✓

Control **SPR 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

Tested via 3 checks

User Access Reviews for Critical Systems	✓
Access to critical systems should be reviewed	✓
Users of critical system should be identified	✓

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 **SPR 33**

Entity has developed a policy 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

Tested via 2 checks

Access control policy should be defined	✓
Access control procedure should be defined	✓

Control **SPR 34**

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

Tested via 2 checks

User access to critical system should be validated by roles	✓
Role based access should be setup	✓

Control **SPR 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

Tested via 3 checks

User Access Reviews for Critical Systems	✓
Access to critical systems should be reviewed	✓
Users of critical system should be identified	✓

Control **SPR 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

Tested via 3 checks

User Access Reviews for Critical Systems	✓
Access to critical systems should be reviewed	✓
Users of critical system should be identified	✓

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 **SPR 1**

Entity has established a policy to define behavioral standards and acceptable business conduct and makes it available to all staff members on the company employee portal

Tested via 1 check

Code of business conduct policy should be defined ✓

Control **SPR 7**

Entity has established an Information Security Awareness training, and its contents are available for all staff on the company employee portal.

Tested via 1 check

Security training provider should be configured ✓

Control **SPR 387**

Entity requires that new staff members complete Information Security Awareness training upon hire

Tested via 1 check

Infosec training should be completed by new staff ✓

Control **SPR 388**

Entity requires that all staff members complete Information Security Awareness training annually

Tested via 1 check

Staff should periodically complete security training ✓

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

Security reminders: Periodic security updates.

INTERNAL CONTROLS AND CHECKS

Control **SPR 46**

Entity ensures that security patches to the operating systems are applied to endpoints with access to critical servers or data in a timely manner

Tested via 1 check

Staff devices should have OS updated ✓

Control **SPR 110**

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

Tested 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 SPR 44

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

Tested via 1 check

Staff devices should have antivirus running	✓

Control SPR 104

Entity has documented guidelines for endpoint security and makes it available for all staff on the company employee portal

Tested via 3 checks

Asset management policy should be defined	✓
Asset management procedure should be defined	✓
Endpoint security policy should be defined	✓

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

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

INTERNAL CONTROLS AND CHECKS

Control SPR 394

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

Tested via 1 check

Audit logs should exist	✓

Control **SPR 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.

Tested via 1 check

Infrastructure provider should be configured ✓

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

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

INTERNAL CONTROLS AND CHECKS

Control **SPR 33**

Entity has developed a policy 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

Tested via 2 checks

Access control policy should be defined ✓

Access control procedure should be defined ✓

Control **SPR 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

Tested via 4 checks

Acceptable usage policy should be defined ✓

Access control policy should be defined ✓

Access control procedure should be defined ✓

Password policy should be defined ✓

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 **SPR 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

Tested via 1 check

Information security policy should be defined ✓

Control **SPR 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.

Tested via 1 check

Customer support page should be available ✓

Control **SPR 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents. This is available to all staff members via the company employee portal.

Tested via 2 checks

Incident management policy should be defined ✓

Incident management procedure should be defined ✓

Control **SPR 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

Tested via 1 check

Incidents should be investigated based on severity ✓

Control **SPR 61**

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

Tested via 1 check

Threat detection system should be enabled ✓

Control **SPR 62**

Entity's Production assets are continuously monitored to generate alerts and take immediate action where necessary

Tested via 1 check

Health of production infrastructure should be monitored ✓

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 **SPR 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

Tested via 1 check

Information security policy should be defined ✓

Control **SPR 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.

Tested via 1 check

Customer support page should be available ✓

Control **SPR 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

Tested via 1 check

Incidents should be investigated based on severity ✓

Control **SPR 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents. This is available to all staff members via the company employee portal.

Tested via 2 checks

Incident management policy should be defined	✓
Incident management procedure should be defined	✓

Control **SPR 112**

Entity has documented guidelines on notifying customers and other stakeholders in case of a breach and makes it available for all staff on the company employee portal

Tested via 1 check

Phi breach notification policy should be defined	✓

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 **SPR 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents. This is available to all staff members via the company employee portal.

Tested via 2 checks

Incident management policy should be defined	✓
Incident management procedure should be defined	✓

Control **SPR 393**

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

Tested via 2 checks

Business continuity plan should be defined	✓
Business continuity & disaster recovery policy should be defined	✓

Control **SPR 392**

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

Tested via 3 checks

Business continuity plan should be defined	✓
Business continuity & disaster recovery policy should be defined	✓
Disaster recovery policy should be defined	✓

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 **SPR 58**

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

Tested via 3 checks

Data backup policy should be defined ✓

Operation security policy should be defined ✓

Operations security procedure should be defined ✓

Control SPR 59

Entity backs-up their production databases periodically

Tested via 1 check

Backup should be enabled on production database ✓

Control SPR 60

Entity's data backups are restored and tested annually

Tested 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 SPR 60

Entity's data backups are restored and tested annually

Tested via 1 check

Data backup restoration ✓

Control **SPR 97**

Entity ensures that the Disaster Recovery Plan is tested periodically and learnings documented

Tested via 1 check

Disaster recovery	✓

Control **SPR 392**

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

Tested via 3 checks

Business continuity plan should be defined	✓
Business continuity & disaster recovery policy should be defined	✓
Disaster recovery policy should be defined	✓

Control **SPR 393**

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

Tested via 2 checks

Business continuity plan should be defined	✓
Business continuity & disaster recovery policy should be defined	✓

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 **SPR 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents. This is available to all staff members via the company employee portal.

Tested via 2 checks

Incident management policy should be defined	✓
Incident management procedure should be defined	✓

Control **SPR 112**

Entity has documented guidelines on notifying customers and other stakeholders in case of a breach and makes it available for all staff on the company employee portal

Tested via 1 check

Phi breach notification policy should be defined	✓

Control **SPR 113**

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

Tested via 1 check

Incidents should be investigated based on severity	✓

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 **SPR 393**

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

Tested via 2 checks

Business continuity plan should be defined	✓
Business continuity & disaster recovery policy should be defined	✓

Control **SPR 392**

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

Tested via 3 checks

Business continuity plan should be defined	✓
Business continuity & disaster recovery policy should be defined	✓
Disaster recovery policy should be defined	✓

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 **SPR 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

Tested via 1 check

Risk assessment should be conducted periodically ✓

Control **SPR 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.

Tested via 1 check

Risk assessment should be conducted periodically ✓

Control **SPR 20**

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

Tested via 1 check

Risk assessment should be conducted periodically ✓

Control **SPR 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 Entity's service commitments and system requirements

Tested via 1 check

Risk assessment & management policy should be defined ✓

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 **SPR 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

Tested via 1 check

Risk assessment should be conducted periodically ✓

Control **SPR 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.

Tested via 1 check

Risk assessment should be conducted periodically ✓

Control **SPR 20**

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

Tested via 1 check

Risk assessment should be conducted periodically ✓

Control **SPR 27**

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

Tested via 1 check

Risk assessment should be reviewed by senior management ✓

Control **SPR 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 Entity's service commitments and system requirements

Tested via 1 check

Risk assessment & management policy should be defined ✓

Control **SPR 63**

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

Tested via 1 check

VAPT exercise should be conducted annually ✓

Control **SPR 55**

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

Tested via 2 checks

Vulnerability should be closed in SLA ✓

Vulnerability scanner should be enabled ✓

Control **SPR 56**

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

Tested 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 **SPR 21**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically ✓

Control **SPR 29**

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

Tested via 1 check

Vendor risk assessment should be reviewed by senior management ✓

Control **SPR 68**

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

Tested via 1 check

Vendor management policy should be defined ✓

Control **SPR 77**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically ✓

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 **SPR 21**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically ✓

Control **SPR 29**

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

Tested via 1 check

Vendor risk assessment should be reviewed by senior management ✓

Control **SPR 68**

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

Tested via 1 check

Vendor management policy should be defined ✓

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 **SPR 381**

Entity has documented guidelines to manage physical and environmental security and makes it available for all staff on the company employee portal

Tested via 2 checks

Physical and environmental security procedure should be defined ✓

Physical & environmental security policy should be defined ✓

Control **SPR 21**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically ✓

Control **SPR 29**

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

Tested via 1 check

Vendor risk assessment should be reviewed by senior management ✓

Control **SPR 68**

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

Tested via 1 check

Vendor management policy should be defined ✓

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 **SPR 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents. This is available to all staff members via the company employee portal.

Tested via 2 checks

Incident management policy should be defined	✓
Incident management procedure should be defined	✓

Control **SPR 392**

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

Tested via 3 checks

Business continuity plan should be defined	✓
Business continuity & disaster recovery policy should be defined	✓
Disaster recovery policy should be defined	✓

Control **SPR 393**

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

Tested via 2 checks

Business continuity plan should be defined	✓
Business continuity & disaster recovery policy should be defined	✓

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 **SPR 381**

Entity has documented guidelines to manage physical and environmental security and makes it available for all staff on the company employee portal

Tested via 2 checks

Physical and environmental security procedure should be defined ✓

Physical & environmental security policy should be defined ✓

Control **SPR 21**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically ✓

Control **SPR 29**

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

Tested via 1 check

Vendor risk assessment should be reviewed by senior management ✓

Control **SPR 68**

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

Tested via 1 check

Vendor management policy should be defined ✓

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 **SPR 21**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically ✓

Control **SPR 29**

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

Tested via 1 check

Vendor risk assessment should be reviewed by senior management ✓

Control **SPR 30**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically ✓

Control **SPR 68**

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

Tested via 1 check

Vendor management policy should be defined ✓

Control **SPR 33**

Entity has developed a policy 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

Tested via 2 checks

Access control policy should be defined ✓

Access control procedure should be defined ✓

Control **SPR 34**

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

Tested via 2 checks

User access to critical system should be validated by roles ✓

Role based access should be setup ✓

Control **SPR 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

Tested via 3 checks

User Access Reviews for Critical Systems	✓
Access to critical systems should be reviewed	✓
Users of critical system should be identified	✓

Control **SPR 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

Tested via 3 checks

User Access Reviews for Critical Systems	✓
Access to critical systems should be reviewed	✓
Users of critical system should be identified	✓

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 **SPR 48**

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

Tested via 1 check

Media disposal policy should be defined	✓

Control **SPR 381**

Entity has documented guidelines to manage physical and environmental security and makes it available for all staff on the company employee portal

Tested via 2 checks

Physical and environmental security procedure should be defined	✓
Physical & environmental security policy should be defined	✓

Control **SPR 31**

Entity has developed a set of policies that establish expected behavior with regard to the Company's control environment.

Tested 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 **SPR 104**

Entity has documented guidelines for endpoint security and makes it available for all staff on the company employee portal

Tested via 3 checks

Asset management policy should be defined	✓

Asset management procedure should be defined ✓

Endpoint security policy should be defined ✓

Control **SPR 44**

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

Tested via 1 check

Staff devices should have antivirus running ✓

Control **SPR 45**

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

Tested via 1 check

Staff devices should have disk encryption enabled ✓

Control **SPR 46**

Entity ensures that security patches to the operating systems are applied to endpoints with access to critical servers or data in a timely manner

Tested via 1 check

Staff devices should have OS updated ✓

Control **SPR 47**

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

Tested via 2 checks

Health of staff devices should be monitored ✓

Staff devices should have screen lock enabled ✓

Control **SPR 48**

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

Tested via 1 check

Media disposal policy should be defined ✓

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 **SPR 44**

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

Tested via 1 check

Staff devices should have antivirus running ✓

Control **SPR 45**

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

Tested via 1 check

Staff devices should have disk encryption enabled	✓

Control **SPR 46**

Entity ensures that security patches to the operating systems are applied to endpoints with access to critical servers or data in a timely manner

Tested via 1 check

Staff devices should have OS updated	✓

Control **SPR 47**

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

Tested via 2 checks

Health of staff devices should be monitored	✓
Staff devices should have screen lock enabled	✓

Control **SPR 48**

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

Tested via 1 check

Media disposal policy should be defined	✓

Control **SPR 104**

Entity has documented guidelines for endpoint security and makes it available for all staff on the company employee portal

Tested via 3 checks

Asset management policy should be defined	✓
Asset management procedure should be defined	✓
Endpoint security policy should be defined	✓

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 **SPR 48**

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

Tested via 1 check

Media disposal policy should be defined	✓

Control **SPR 105**

Entity has documented guidelines on Acceptable Usage of Entity's assets and makes it available for all staff on the company employee portal

Tested via 1 check

Acceptable usage policy should be defined	✓

Control **SPR 382**

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

Tested via 1 check

Data classification policy should be defined	✓

Control **SPR 70**

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

Tested via 1 check

Data classification policy should be defined	✓

Control **SPR 69**

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

Tested via 2 checks

Confidentiality policy should be defined	✓
Information security policy should be defined	✓

Control **SPR 390**

Entity maintains the inventory of endpoint assets and segregates assets with access to critical data from the others

Tested via 2 checks

Asset management procedure should be defined	✓
Staff devices health should be monitored regularly	✓

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 **SPR 48**

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

Tested via 1 check

Media disposal policy should be defined ✓

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 **SPR 70**

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

Tested via 1 check

Data classification policy should be defined ✓

Control **SPR 382**

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

Tested via 1 check

Data classification policy should be defined ✓

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 **SPR 70**

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

Tested via 1 check

Data classification policy should be defined ✓

Control **SPR 71**

Entity has a documented policy that establishes guidelines for Data Retention and makes it available for all staff on the company employee portal

Tested via 1 check

Data retention policy should be defined ✓

Control **SPR 72**

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

Tested via 1 check

Data protection policy should be defined ✓

Control **SPR 48**

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

Tested via 1 check

Media disposal policy should be defined ✓

Control **SPR 104**

Entity has documented guidelines for endpoint security and makes it available for all staff on the company employee portal

Tested via 3 checks

Asset management policy should be defined ✓

Asset management procedure should be defined ✓

Endpoint security policy should be defined ✓

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 **SPR 58**

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

Tested via 3 checks

Data backup policy should be defined	✓
Operation security policy should be defined	✓
Operations security procedure should be defined	✓

Control **SPR 59**

Entity backs-up their production databases periodically

Tested via 1 check

Backup should be enabled on production database	✓

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 **SPR 33**

Entity has developed a policy 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

Tested via 2 checks

Access control policy should be defined	✓

Access control procedure should be defined	✓

Control **SPR 34**

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

Tested via 2 checks

User access to critical system should be validated by roles	✓
Role based access should be setup	✓

Control **SPR 35**

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

Tested via 0 checks

Control **SPR 37**

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

Tested via 3 checks

User Access Reviews for Critical Systems	✓
Access to critical systems should be reviewed	✓
Users of critical system should be identified	✓

Control **SPR 38**

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

Tested via 1 check

Public access for infra assets should be restricted	✓

Control **SPR 39**

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

Tested via 4 checks

MFA Enforced by System Configuration	✓
Office365 User MFA Status	✓
Password Complexity Enforced by System Configuration	✓
Users should have MFA enabled for login	✓

Control **SPR 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

Tested via 3 checks

User Access Reviews for Critical Systems	✓
Access to critical systems should be reviewed	✓
Users of critical system should be identified	✓

Control **SPR 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

Tested via 3 checks

User Access Reviews for Critical Systems	✓
Access to critical systems should be reviewed	✓
Users of critical system should be identified	✓

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 **SPR 39**

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

Tested via 4 checks

MFA Enforced by System Configuration	✓
Office365 User MFA Status	✓
Password Complexity Enforced by System Configuration	✓
Users should have MFA enabled for login	✓

Control **SPR 37**

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

Tested via 3 checks

User Access Reviews for Critical Systems	✓
Access to critical systems should be reviewed	✓
Users of critical system should be identified	✓

Control **SPR 38**

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

Tested via 1 check

Public access for infra assets should be restricted	✓

Control **SPR 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

Tested via 3 checks

User Access Reviews for Critical Systems	✓
Access to critical systems should be reviewed	✓
Users of critical system should be identified	✓

Control **SPR 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

Tested via 3 checks

User Access Reviews for Critical Systems	✓
Access to critical systems should be reviewed	✓
Users of critical system should be identified	✓

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 **SPR 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents. This is available to all staff members via the company employee portal.

Tested via 2 checks

Incident management policy should be defined	✓
Incident management procedure should be defined	✓

Control **SPR 392**

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

Tested via 3 checks

Business continuity plan should be defined	✓
Business continuity & disaster recovery policy should be defined	✓
Disaster recovery policy should be defined	✓

Control **SPR 393**

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

Tested via 2 checks

Business continuity plan should be defined	✓
Business continuity & disaster recovery policy should be defined	✓

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 **SPR 47**

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

Tested via 2 checks

Health of staff devices should be monitored	✓
Staff devices should have screen lock enabled	✓

Control **SPR 109**

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

Tested 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 **SPR 45**

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

Tested via 1 check

Staff devices should have disk encryption enabled ✓

Control **SPR 49**

All production database[s] that store customer data are encrypted at rest.

Tested via 1 check

Data at rest should be encrypted ✓

Control **SPR 51**

User access to the entity's application is secured using https (TLS algorithm) and industry standard encryption.

Tested via 1 check

Production systems should be secured with HTTPS ✓

Control **SPR 106**

Entity has a documented policy to manage encryption and makes it available for all staff on the company employee portal

Tested via 1 check

Encryption policy should be defined ✓

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 **SPR 61**

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

Tested via 1 check

Threat detection system should be enabled ✓

Control **SPR 62**

Entity's Production assets are continuously monitored to generate alerts and take immediate action where necessary

Tested via 1 check

Health of production infrastructure should be monitored ✓

Control **SPR 394**

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

Tested via 1 check

Audit logs should exist ✓

164.312(c)(1)

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

INTERNAL CONTROLS AND CHECKS

Control **SPR 71**

Entity has a documented policy that establishes guidelines for Data Retention and makes it available for all staff on the company employee portal

Tested via 1 check

Data retention policy should be defined ✓

Control **SPR 72**

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

Tested via 1 check

Data protection policy should be defined ✓

Control **SPR 70**

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

Tested via 1 check

Data classification policy should be defined ✓

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 **SPR 61**

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

Tested via 1 check

Threat detection system should be enabled ✓

Control **SPR 63**

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

Tested via 1 check

VAPT exercise should be conducted annually ✓

Control **SPR 62**

Entity's Production assets are continuously monitored to generate alerts and take immediate action where necessary

Tested via 1 check

Health of production infrastructure should be monitored ✓

Control **SPR 56**

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

Tested via 1 check

Vulnerability should be closed in SLA	✓

Control **SPR 55**

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

Tested 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 **SPR 33**

Entity has developed a policy 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

Tested via 2 checks

Access control policy should be defined	✓
Access control procedure should be defined	✓

Control **SPR 34**

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

Tested via 2 checks

User access to critical system should be validated by roles	✓
Role based access should be setup	✓

Control **SPR 35**

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

Tested via 0 checks

Control **SPR 37**

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

Tested via 3 checks

User Access Reviews for Critical Systems	✓
Access to critical systems should be reviewed	✓
Users of critical system should be identified	✓

Control **SPR 38**

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

Tested via 1 check

Public access for infra assets should be restricted	✓

Control **SPR 39**

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

Tested via 4 checks

MFA Enforced by System Configuration	✓
Office365 User MFA Status	✓
Password Complexity Enforced by System Configuration	✓
Users should have MFA enabled for login	✓

Control **SPR 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

Tested via 3 checks

User Access Reviews for Critical Systems	✓
Access to critical systems should be reviewed	✓
Users of critical system should be identified	✓

Control **SPR 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

Tested via 3 checks

User Access Reviews for Critical Systems	✓

Access to critical systems should be reviewed ✓

Users of critical system should be identified ✓

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 **SPR 70**

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

Tested via 1 check

Data classification policy should be defined ✓

Control **SPR 69**

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

Tested via 2 checks

Confidentiality policy should be defined ✓

Information security policy should be defined ✓

Control **SPR 106**

Entity has a documented policy to manage encryption and makes it available for all staff on the company employee portal

Tested via 1 check

Encryption policy should be defined ✓

Control **SPR 49**

All production database[s] that store customer data are encrypted at rest.

Tested via 1 check

Data at rest should be encrypted ✓

Control **SPR 51**

User access to the entity's application is secured using https (TLS algorithm) and industry standard encryption.

Tested via 1 check

Production systems should be secured with HTTPS ✓

Control **SPR 45**

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

Tested via 1 check

Staff devices should have disk encryption enabled ✓

Control **SPR 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

Tested 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 **SPR 106**

Entity has a documented policy to manage encryption and makes it available for all staff on the company employee portal

Tested via 1 check

Encryption policy should be defined ✓

Control **SPR 7**

Entity has established an Information Security Awareness training, and its contents are available for all staff on the company employee portal.

Tested via 1 check

Security training provider should be configured ✓

Control **SPR 6**

Entity requires that new staff members review and acknowledge relevant company policies, including the code of business conduct, as part of their onboarding. This ensures they understand their responsibilities and are willing to comply with them

Tested via 1 check

Policies should be acknowledged by new staff ✓

164.312(e)(2)(ii)

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

INTERNAL CONTROLS AND CHECKS

Control **SPR 45**

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

Tested via 1 check

Staff devices should have disk encryption enabled ✓

Control **SPR 49**

All production database[s] that store customer data are encrypted at rest.

Tested via 1 check

Data at rest should be encrypted ✓

Control **SPR 51**

User access to the entity's application is secured using https (TLS algorithm) and industry standard encryption.

Tested via 1 check

Production systems should be secured with HTTPS ✓

Control **SPR 106**

Entity has a documented policy to manage encryption and makes it available for all staff on the company employee portal

Tested via 1 check

Encryption policy should be defined ✓

164.314

Organizational requirements

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 **SPR 21**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically ✓

Control **SPR 29**

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

Tested via 1 check

Vendor risk assessment should be reviewed by senior management ✓

Control **SPR 30**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically ✓

Control **SPR 68**

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

Tested via 1 check

Vendor management policy should be defined ✓

Control **SPR 77**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically ✓

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 **SPR 21**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically ✓

Control **SPR 29**

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

Tested via 1 check

Vendor risk assessment should be reviewed by senior management ✓

Control **SPR 30**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically ✓

Control **SPR 77**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically ✓

Control **SPR 68**

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

Tested via 1 check

Vendor management policy should be defined ✓

Control **SPR 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

Tested via 1 check

Records of Processing Activities (ROPA) & Data flow map ✓

Control **SPR 76**

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

Tested via 1 check

Data consent using cookie banner ✓

Control **SPR 79**

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

Tested via 1 check

Risk assessment should be conducted periodically ✓

Control **SPR 80**

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

Tested via 1 check

Data Subject Access Requests (SARs) Report ✓

Control **SPR 95**

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

Tested via 2 checks

Acceptable usage policy should be defined ✓

Endpoint security policy should be defined ✓

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 **SPR 21**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically ✓

Control **SPR 29**

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

Tested via 1 check

Vendor risk assessment should be reviewed by senior management ✓

Control **SPR 30**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically ✓

Control **SPR 68**

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

Tested via 1 check

Vendor management policy should be defined ✓

Control **SPR 77**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically ✓

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 **SPR 21**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically ✓

Control **SPR 29**

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

Tested via 1 check

Vendor risk assessment should be reviewed by senior management ✓

Control **SPR 30**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically ✓

Control **SPR 68**

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

Tested via 1 check

Vendor management policy should be defined ✓

Control **SPR 77**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically ✓

Control **SPR 97**

Entity ensures that the Disaster Recovery Plan is tested periodically and learnings documented

Tested via 1 check

Disaster recovery ✓

Control **SPR 98**

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

Tested via 1 check

Management review of contractual obligations ✓

Control **SPR 100**

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

Tested via 1 check

Critical Infrastructure assets should be identified ✓

Control **SPR 143**

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

Tested via 0 checks

Control **SPR 144**

Entity's senior management reviews and approves the Privacy Policy and Terms of Service periodically

Tested via 1 check

Review of the privacy policy ✓

Control **SPR 141**

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

Tested via 2 checks

Staff devices should have disk encryption enabled ✓

Health of staff devices should be monitored ✓

Control **SPR 64**

Entity has a documented policy and procedure to manage changes to its operating environment that includes critical information. Such documentation is available to all relevant Staff Members via the company employee portal

Tested via 4 checks

Change management policy should be defined	✓
Operations security procedure should be defined	✓
System acquisition and development lifecycle policy should be defined	✓
Sdlc procedure should be defined	✓

Control SPR 65

Entity uses a change management system to track, review and log all changes to the application code.

Tested via 2 checks

Change management repos should be classified	✓
Change management source should be configured	✓

Control SPR 66

Entity ensures that all planned changes undergo a review and approval process as per the guidelines documented in the policy and procedure defined to manage changes

Tested via 5 checks

Changes to production code should be reviewed by peers	✓
Peer review should be enabled in control systems	✓
Change requests should be reviewed by peers	✓
Operations security procedure should be defined	✓
Sdlc procedure should be defined	✓

Control **SPR 9**

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

Tested via 1 check

Staff Performance Evaluations ✓

Control **SPR 11**

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

Tested via 1 check

Health of production infrastructure should be monitored ✓

Control **SPR 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.

Tested via 1 check

Risk assessment should be conducted periodically ✓

Control **SPR 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

Tested via 1 check

Internal Audit ✓

Control **SPR 49**

All production database[s] that store customer data are encrypted at rest.

Tested via 1 check

Data at rest should be encrypted ✓

Control **SPR 52**

Entity maintains an inventory of infrastructure assets and segregates production assets from its staging/development assets

Tested via 1 check

Critical Infrastructure assets should be identified ✓

Control **SPR 59**

Entity backs-up their production databases periodically

Tested via 1 check

Backup should be enabled on production database ✓

Control **SPR 62**

Entity's Production assets are continuously monitored to generate alerts and take immediate action where necessary

Tested via 1 check

Health of production infrastructure should be monitored ✓

Control **SPR 69**

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

Tested via 2 checks

Confidentiality policy should be defined	✓
Information security policy should be defined	✓

Control **SPR 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

Tested via 1 check

Vendor risk assessment should be conducted periodically	✓

Control **SPR 114**

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

Tested via 1 check

Privacy officer should be assigned	✓

Control **SPR 383**

Entity requires that all staff members complete Information Security Awareness training annually.

Tested via 1 check

Staff should periodically complete security training	✓

Control **SPR 387**

Entity requires that new staff members complete Information Security Awareness training upon hire

Tested via 1 check

Infosec training should be completed by new staff	✓

Control **SPR 388**

Entity requires that all staff members complete Information Security Awareness training annually

Tested via 1 check

Staff should periodically complete security training	✓

Control **SPR 390**

Entity maintains the inventory of endpoint assets and segregates assets with access to critical data from the others

Tested via 2 checks

Asset management procedure should be defined	✓
Staff devices health should be monitored regularly	✓

Control **SPR 389**

Entity maintains and periodically reviews the inventory of systems which are critical to security commitments and requirements

Tested via 3 checks

Internal Audit	✓
Asset management policy should be defined	✓
Asset management procedure should be defined	✓

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 **SPR 21**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically ✓

Control **SPR 29**

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

Tested via 1 check

Vendor risk assessment should be reviewed by senior management ✓

Control **SPR 30**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically ✓

Control **SPR 68**

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

Tested via 1 check

Vendor management policy should be defined ✓

Control **SPR 77**

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

Tested via 1 check

Vendor risk assessment should be conducted periodically ✓

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 **SPR 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents. This is available to all staff members via the company employee portal.

Tested via 2 checks

Incident management policy should be defined ✓

Incident management procedure should be defined ✓

Control **SPR 112**

Entity has documented guidelines on notifying customers and other stakeholders in case of a breach and makes it available for all staff on the company employee portal

Tested via 1 check

Phi breach notification policy should be defined ✓

Control **SPR 113**

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

Tested via 1 check

Incidents should be investigated based on severity ✓

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 **SPR 24**

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

Tested via 1 check

Policies should be reviewed by senior management ✓

Control **SPR 31**

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

Tested via 1 check

Org policy should be defined ✓

Control **SPR 111**

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

Tested 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 **SPR 24**

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

Tested via 1 check

Policies should be reviewed by senior management ✓

Control **SPR 31**

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

Tested 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 **SPR 31**

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

Tested via 1 check

Org policy should be defined ✓

Control **SPR 24**

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

Tested 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 **SPR 71**

Entity has a documented policy that establishes guidelines for Data Retention and makes it available for all staff on the company employee portal

Tested via 1 check

Data retention policy should be defined ✓

Control **SPR 111**

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

Tested 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 **SPR 6**

Entity requires that new staff members review and acknowledge relevant company policies, including the code of business conduct, as part of their onboarding. This ensures they understand their responsibilities and are willing to comply with them

Tested via 1 check

Policies should be acknowledged by new staff ✓

Control **SPR 12**

Entity requires that all staff members review and acknowledge company policies annually

Tested via 1 check

Staff should periodically acknowledge policies ✓

Control **SPR 13**

Entity makes all policies and procedures available to all staff members via the company employee portal

Tested via 0 checks

Control **SPR 31**

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

Tested via 1 check

Org policy should be defined ✓

Control **SPR 24**

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

Tested 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 **SPR 112**

Entity has documented guidelines on notifying customers and other stakeholders in case of a breach and makes it available for all staff on the company employee portal

Tested via 1 check

Phi breach notification policy should be defined ✓

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 **SPR 112**

Entity has documented guidelines on notifying customers and other stakeholders in case of a breach and makes it available for all staff on the company employee portal

Tested via 1 check

Phi breach notification policy should be defined ✓

Control **SPR 113**

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

Tested via 1 check

Incidents should be investigated based on severity ✓

Control **SPR 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents. This is available to all staff members via the company employee portal.

Tested via 2 checks

Incident management policy should be defined ✓

Incident management procedure should be defined ✓

Control **SPR 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

Tested 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 **SPR 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents. This is available to all staff members via the company employee portal.

Tested via 2 checks

Incident management policy should be defined	✓
Incident management procedure should be defined	✓

Control **SPR 112**

Entity has documented guidelines on notifying customers and other stakeholders in case of a breach and makes it available for all staff on the company employee portal

Tested via 1 check

Phi breach notification policy should be defined	✓

Control **SPR 113**

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

Tested via 1 check

Incidents should be investigated based on severity	✓

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 **SPR 6**

Entity requires that new staff members review and acknowledge relevant company policies, including the code of business conduct, as part of their onboarding. This ensures they understand their responsibilities and are willing to comply with them

Tested via 1 check

Policies should be acknowledged by new staff ✓

Control **SPR 12**

Entity requires that all staff members review and acknowledge company policies annually

Tested via 1 check

Staff should periodically acknowledge policies ✓

Control **SPR 112**

Entity has documented guidelines on notifying customers and other stakeholders in case of a breach and makes it available for all staff on the company employee portal

Tested via 1 check

Phi breach notification policy should be defined ✓

Control **SPR 113**

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

Tested via 1 check

Incidents should be investigated based on severity ✓

Control **SPR 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents. This is available to all staff members via the company employee portal.

Tested via 2 checks

Incident management policy should be defined	✓
Incident management procedure should be defined	✓

Control **SPR 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

Tested 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 **SPR 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents. This is available to all staff members via the company employee portal.

Tested via 2 checks

Incident management policy should be defined ✓

Incident management procedure should be defined ✓

Control SPR 112

Entity has documented guidelines on notifying customers and other stakeholders in case of a breach and makes it available for all staff on the company employee portal

Tested via 1 check

Phi breach notification policy should be defined ✓

Control SPR 113

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

Tested via 1 check

Incidents should be investigated based on severity ✓

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 SPR 112

Entity has documented guidelines on notifying customers and other stakeholders in case of a breach and makes it available for all staff on the company employee portal

Tested via 1 check

Phi breach notification policy should be defined ✓

Control **SPR 53**

Entity has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents. This is available to all staff members via the company employee portal.

Tested via 2 checks

Incident management policy should be defined ✓

Incident management procedure should be defined ✓

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.