

# HIPAA Gap Assessment from Vanta

FORRECORD



**RECORD**

# Administrative safeguards

164.308(a)(1)(i)

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

1 CONTROL

## ▶ Security violations managed

✓ COMPLETE

The company has implemented policies and procedures to prevent, detect, contain, and correct security violations. If the company has committed to an SLA for a security violation, the corrective action is completed within that SLA.

5 TESTS

**Company has an approved Incident Response Plan:** Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

**Company has an approved Incident Response Plan HIPAA Addendum with Breach Notification Procedures:** Verifies that a Incident Response Plan HIPAA Addendum with Breach Notification Procedures has been created and approved within Vanta. ✓

**Company has an approved Information Security Policy (AUP):** Verifies that a Information Security Policy (AUP) has been created and approved within Vanta. ✓

**Company has an approved Operations Security Policy:** Verifies that a Operations Security Policy has been created and approved within Vanta. ✓

**Employees agree to Incident Response Plan HIPAA Addendum with Breach Notification Procedures:** Verifies that all relevant employees have agreed to the Incident Response Plan HIPAA Addendum with Breach Notification Procedures. ✓

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.

1 CONTROL

▶ Risks analyzed

✓ COMPLETE

The company has conducted an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held in its system.

2 TESTS

**Company has an approved Risk Management Policy:** Verifies that a Risk Management Policy has been created and approved within Vanta. ✓

**HIPAA risks are reviewed annually:** Verifies that at least one Privacy-related risk is included in a valid snapshot of the risk register (i.e. a snapshot taken in the past year) ✓

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

1 CONTROL

▶ Risks managed

✓ COMPLETE

The company has implemented security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the HIPAA security general requirements (described in § 164.306(a)).

2 TESTS

**Company has an approved Risk Management Policy:** Verifies that a Risk Management Policy has been created and approved within Vanta. ✓

**HIPAA risks are reviewed annually:** Verifies that at least one Privacy-related risk is included in a valid snapshot of the risk register (i.e. a snapshot taken in the past year) ✓

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.

1 CONTROL

▶ Sanction policy applied

✓ COMPLETE

The company applies appropriate sanctions against workforce members who fail to comply with the security policies and procedures.

3 TESTS

**Company has an approved HIPAA Compliance Policy:** Verifies that a HIPAA Compliance Policy has been created and approved within Vanta. ✓

**Company has an approved Information Security Policy (AUP):** Verifies that a Information Security Policy (AUP) has been created and approved within Vanta. ✓

**Employees agree to HIPAA Compliance Policy:** Verifies that all relevant employees have agreed to the HIPAA Compliance Policy. ✓

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.

1 CONTROL

▶ Information system activity reviewed

✓ COMPLETE

The company has implemented procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

7 TESTS

**Company has an approved Access Control Policy:** Verifies that a Access Control Policy has been created and approved within Vanta. ✓

**Company has an approved Incident Response Plan:** Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

**Company has an approved Incident Response Plan HIPAA Addendum with Breach Notification Procedures:** Verifies that a Incident Response Plan HIPAA Addendum with Breach Notification Procedures has been created and approved within Vanta. ✓

**Company has an approved Operations Security Policy:** Verifies that a Operations Security Policy has been created and approved within Vanta. ✓

**Records of security issues being assigned to owners:** Verifies that all tasks in the linked task tracker that are labeled with a `security` tag have an owner assigned within the task tracker. ✓

**Security issues assigned priorities:** Verifies that all tasks in the linked task tracker that are labeled with a `security` have a priority assigned within the task tracker. ✓

**Records of security issues being tracked:** Verifies that at least one task in the linked task tracker is labeled with a `security` tag. ✓

2 DOCUMENTS

**Incident report or root cause analysis** ✓

**Enabled automated log alerting** ✓

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.

2 CONTROLS

▶ HIPAA security officer

✓ COMPLETE

The company has implemented policies and procedures to address the final disposition of electronic Protected Health Information (ePHI), and/or the hardware or electronic media on which it is stored.

1 TEST

**HIPAA Security Officer is an active employee:** Verifies that a HIPAA Security Officer has been designated in Vanta and that the officer is an active employee.

✓

▶ Security responsibility assigned

✓ COMPLETE

The company has identified a security official to be responsible for the development and implementation of the policies and procedures required by the HIPAA Security rules for the company.

2 TESTS

**Company has an approved HIPAA Compliance Policy:** Verifies that a HIPAA Compliance Policy has been created and approved within Vanta.

✓

**Employees agree to HIPAA Compliance Policy:** Verifies that all relevant employees have agreed to the HIPAA Compliance Policy.

✓

164.308(a)(3)(i)

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

1 CONTROL

▶ Workforce security implemented

✓ COMPLETE

The company has implemented policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information (ePHI), and to prevent those workforce members who do not have access from obtaining access to ePHI.

1 TEST

**Company has an approved Access Control Policy:** Verifies that a Access Control Policy has been created and approved within Vanta.



1 DOCUMENT

**Access request ticket and history**



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.

1 CONTROL

▶ Workforce authorized and/or supervised

✓ COMPLETE

The company has implemented procedures for the authorization and/or supervision of workforce members who work with electronic protected health information (ePHI) or in locations where it might be accessed.

1 TEST

**Company has an approved Access Control Policy:** Verifies that a Access Control Policy has been created and approved within Vanta.



1 DOCUMENT

**Access request ticket and history**



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.

1 CONTROL

▶ Workforce clearance procedures implemented

✓ COMPLETE

The company has implemented procedures to determine that the access of a workforce member to electronic protected health information (ePHI) is appropriate.

1 TEST

**Company has an approved Access Control Policy:** Verifies that a Access Control Policy has been created and approved within Vanta.

✓

1 DOCUMENT

**Access request ticket and history**

✓

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.

1 CONTROL



▶ Termination procedures established

✓ COMPLETE

The company has implement procedures for terminating access to electronic protected health information (ePHI) when the employment of a workforce member ends or as required when access is no longer appropriate.

6 TESTS

- Company has an approved Access Control Policy:** Verifies that a Access Control Policy has been created and approved within Vanta. ✓
- Datadog accounts deprovisioned when employees leave:** Verifies that Datadog accounts linked to removed users are removed. ✓
- GitHub accounts deprovisioned when employees leave:** Verifies that GitHub accounts linked to removed users are removed. ✓
- Heroku accounts deprovisioned when employees leave:** Verifies that Heroku accounts linked to removed users are removed. ✓
- Slack accounts deprovisioned when employees leave:** Verifies that Slack accounts linked to removed users are removed. ✓
- Offboarding completed for ex-employees within SLA:** Verifies that all ex-employees linked to Vanta have had their accounts deprovisioned and offboarding marked as completed. ✓

2 DOCUMENTS

- Employee exit process** ✓
- Employee termination security policy** ✓

164.308(a)(4)(i)

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

1 CONTROL

▶ Information access managed

✓ COMPLETE

The company has implemented policies and procedures for authorizing access to electronic protected health information (ePHI) that are consistent with the applicable privacy rule requirements (subpart E).

1 TEST

**Company has an approved Access Control Policy:** Verifies that a Access Control Policy has been created and approved within Vanta.



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.

1 CONTROL

▶ Access authorized

✓ COMPLETE

The company has implemented policies and procedures for granting access to electronic protected health information (for example, through access to a workstation, transaction, program, process, or other mechanism).

1 TEST

**Company has an approved Access Control Policy:** Verifies that a Access Control Policy has been created and approved within Vanta.



1 DOCUMENT

**Access request ticket and history**



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.

1 CONTROL

▶ Access established, reviewed and modified

✓ COMPLETE

The company has implemented policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

7 TESTS

**Company has an approved Access Control Policy:** Verifies that a Access Control Policy has been created and approved within Vanta. ✓

**Datadog accounts associated with users:** Verifies that all Datadog accounts have been linked to users within Vanta. ✓

**GitHub accounts associated with users:** Verifies that all GitHub accounts have been linked to users within Vanta. ✓

**Heroku accounts associated with users:** Verifies that all Heroku accounts have been linked to users within Vanta. ✓

**HR accounts associated with users:** Verifies that all HR accounts have been linked to users within Vanta. ✓

**User activity and API use is tracked (Heroku):** This feature is built into Heroku. ✓

**Slack accounts associated with users:** Verifies that all Slack accounts have been linked to users within Vanta. ✓

1 DOCUMENT

**Access request ticket and history** ✓

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.

1 CONTROL

▶ Security awareness training implemented

✓ COMPLETE

The company has implemented a security awareness and training program for all members of its workforce, including management.

5 TESTS

**Company has an approved Human Resource Security Policy:** Verifies that a Human Resource Security Policy has been created and approved within Vanta. ✓

**HIPAA security awareness training selected:** Verifies that a HIPAA security awareness training program has been selected within Vanta. ✓

**HIPAA security awareness training records tracked:** Verifies that all relevant employees have uploaded documentation indicating that they have completed HIPAA security training. ✓

**Security awareness training selected:** Verifies that a security awareness training program has been selected within Vanta. ✓

**General security awareness training records tracked:** Verifies that all relevant employees have uploaded documentation indicating that they have completed general security training. ✓

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

Security reminders: Periodic security updates.

1 CONTROL

▶ Security reminders updated

✓ COMPLETE

The company conducts periodic security updates.

2 DOCUMENTS

**Public change log or release notes** ✓

**Internal communication for system updates** ✓

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

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

1 CONTROL

▶ Malicious software protection implemented ✓ COMPLETE

The company has implemented procedures for guarding against, detecting, and reporting malicious software.

1 TEST

**Company has an approved Operations Security Policy:** Verifies that a Operations Security Policy has been created and approved within Vanta. ✓

---

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

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

---

1 CONTROL

▶ Log-ins monitored ✓ COMPLETE

The company has implemented procedures for monitoring log-in attempts and reporting discrepancies.

1 TEST

**User activity and API use is tracked (Heroku):** This feature is built into Heroku. ✓

---

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

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

---

1 CONTROL

▶ Passwords managed ✓ COMPLETE

The company has implemented procedures for creating, changing, and safeguarding passwords.

3 TESTS

**Company has an approved Access Control Policy:** Verifies that a Access Control Policy has been created and approved within Vanta. ✓

**Company has an approved Information Security Policy (AUP):** Verifies that a Information Security Policy (AUP) has been created and approved within Vanta. ✓

**Password manager records:** Verifies that all employee workstations with the Vanta Agent installed have a password manager installed. ✓

---

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

## 1 CONTROL

▶ Security incident procedures implemented

✓ COMPLETE

The company has implemented policies and procedures to address security incidents.

## 8 TESTS

**Company has an approved Incident Response Plan:** Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

**Company has an approved Incident Response Plan HIPAA Addendum with Breach Notification Procedures:** Verifies that a Incident Response Plan HIPAA Addendum with Breach Notification Procedures has been created and approved within Vanta. ✓

**Company has an approved Information Security Policy (AUP):** Verifies that a Information Security Policy (AUP) has been created and approved within Vanta. ✓

**Employees agree to Incident Response Plan HIPAA Addendum with Breach Notification Procedures:** Verifies that all relevant employees have agreed to the Incident Response Plan HIPAA Addendum with Breach Notification Procedures. ✓

**Records of security issues being assigned to owners:** Verifies that all tasks in the linked task tracker that are labeled with a `security` tag have an owner assigned within the task tracker. ✓

**Security issues assigned priorities:** Verifies that all tasks in the linked task tracker that are labeled with a `security` have a priority assigned within the task tracker. ✓

**Records of security issues being tracked:** Verifies that at least one task in the linked task tracker is labeled with a `security` tag. ✓

**P3 security issues resolved:** Verifies that all tasks in the linked task tracker labeled with a security and p3 tag are marked as complete. ✓

## 1 DOCUMENT

**Incident report or root cause analysis**

✓

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.

---

1 CONTROL

▶ Security incidents identified and reported

✓ COMPLETE

The company identifies and responds to suspected or known security incidents, mitigates, to the extent practicable, harmful effects of security incidents that are known to the company, and documents security incidents and their outcomes.

6 TESTS

**Company has an approved Incident Response Plan:** Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

**Company has an approved Incident Response Plan HIPAA Addendum with Breach Notification Procedures:** Verifies that a Incident Response Plan HIPAA Addendum with Breach Notification Procedures has been created and approved within Vanta. ✓

**Company has an approved Information Security Policy (AUP):** Verifies that a Information Security Policy (AUP) has been created and approved within Vanta. ✓

**Records of security issues being assigned to owners:** Verifies that all tasks in the linked task tracker that are labeled with a `security` tag have an owner assigned within the task tracker. ✓

**Security issues assigned priorities:** Verifies that all tasks in the linked task tracker that are labeled with a `security` have a priority assigned within the task tracker. ✓

**Records of security issues being tracked:** Verifies that at least one task in the linked task tracker is labeled with a `security` tag. ✓

1 DOCUMENT

**Incident report or root cause analysis**

✓

---

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.

---

1 CONTROL

▶ Contingency plan established

✓ COMPLETE

The company has established (and implements 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 electronic Protected Health Information (ePHI).

2 TESTS

**Company has an approved Business Continuity and Disaster Recovery Plan:** Verifies that a Business Continuity and Disaster Recovery Plan has been created and approved within Vanta. ✓

**Employees agree to Business Continuity and Disaster Recovery Plan:** Verifies that all relevant employees have agreed to the Business Continuity and Disaster Recovery Plan. ✓

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

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

1 CONTROL

▶ Data backup plan implemented

✓ COMPLETE

The company has established and implements procedures to create and maintain retrievable exact copies of electronic protected health information (ePHI).

2 TESTS

**Company has an approved Operations Security Policy:** Verifies that a Operations Security Policy has been created and approved within Vanta. ✓

**Daily database backups (Heroku):** Verifies that all Heroku databases are backed up daily. This feature is automatically provided by Heroku Postgres plans on at least the Standard tier. ✓

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

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

1 CONTROL



▶ Disaster recovery plan established

✓ COMPLETE

The company has established (and implements as needed) procedures to restore any loss of data.

3 TESTS

**Company has an approved Business Continuity and Disaster Recovery Plan:** Verifies that a Business Continuity and Disaster Recovery Plan has been created and approved within Vanta. ✓

**Company has an approved Operations Security Policy:** Verifies that a Operations Security Policy has been created and approved within Vanta. ✓

**Employees agree to Business Continuity and Disaster Recovery Plan:** Verifies that all relevant employees have agreed to the Business Continuity and Disaster Recovery Plan. ✓

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.

1 CONTROL

▶ Emergency mode operation plan established

✓ COMPLETE

The company has established (and implements as needed) procedures to enable the continuation of critical business processes for the protection and security of electronic Protected Health Information (ePHI) while operating in emergency mode.

2 TESTS

**Company has an approved Business Continuity and Disaster Recovery Plan:** Verifies that a Business Continuity and Disaster Recovery Plan has been created and approved within Vanta. ✓

**Employees agree to Business Continuity and Disaster Recovery Plan:** Verifies that all relevant employees have agreed to the Business Continuity and Disaster Recovery Plan. ✓

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

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

1 CONTROL

▶ Contingency plan tested and revised

✓ COMPLETE

The company has implemented procedures for periodic testing and revision of contingency plans.

2 TESTS

**Company has an approved Business Continuity and Disaster Recovery Plan:** Verifies that a Business Continuity and Disaster Recovery Plan has been created and approved within Vanta. ✓

**Employees agree to Business Continuity and Disaster Recovery Plan:** Verifies that all relevant employees have agreed to the Business Continuity and Disaster Recovery Plan. ✓

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.

1 CONTROL

▶ Application and data criticality analyzed

✓ COMPLETE

The company assesses the relative criticality of specific applications and data in support of other contingency plan components.

2 TESTS

**Company has an approved Risk Management Policy:** Verifies that a Risk Management Policy has been created and approved within Vanta. ✓

**HIPAA risks are reviewed annually:** Verifies that at least one Privacy-related risk is included in a valid snapshot of the risk register (i.e. a snapshot taken in the past year) ✓

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.

1 CONTROL

▶ Security controls evaluated

✓ COMPLETE

The company performs a periodic technical and nontechnical evaluation, based initially upon the HIPAA security rule, and subsequently, in response to environmental or operational changes affecting the security of electronic Protected Health Information (ePHI), establishes the extent to which the company's security policies and procedures meet the requirements of the HIPAA security rule (subpart C).

6 TESTS

**Company has an approved Risk Management Policy:** Verifies that a Risk Management Policy has been created and approved within Vanta. ✓

**HIPAA risks are reviewed annually:** Verifies that at least one Privacy-related risk is included in a valid snapshot of the risk register (i.e. a snapshot taken in the past year) ✓

**Records of penetration testing:** Verifies that a periodic penetration test has been conducted recently and that evidence of that test has been uploaded to Vanta. ✓

**Records of security issues being assigned to owners:** Verifies that all tasks in the linked task tracker that are labeled with a `security` tag have an owner assigned within the task tracker. ✓

**Security issues assigned priorities:** Verifies that all tasks in the linked task tracker that are labeled with a `security` have a priority assigned within the task tracker. ✓

**Records of security issues being tracked:** Verifies that at least one task in the linked task tracker is labeled with a `security` tag. ✓

3 DOCUMENTS

**Penetration test report** ✓

**Sample of remediated vulnerabilities** ✓

**Vulnerability scan** ✓

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.

1 CONTROL

▶ Business associate contracts with vendors established ✓ COMPLETE

The company, as a covered entity, permits a business associate to create, receive, maintain, or transmit electronic Protected Health Information (ePHI) on the company's behalf only if it can obtain satisfactory assurances, in accordance with company policies, that the business associate will appropriately safeguard the information.

2 TESTS

**Company has an approved HIPAA Compliance Policy:** Verifies that a HIPAA Compliance Policy has been created and approved within Vanta. ✓

**Employees agree to HIPAA Compliance Policy:** Verifies that all relevant employees have agreed to the HIPAA Compliance Policy. ✓

1 DOCUMENT

**Business associate agreement template** ✓

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.

1 CONTROL

▶ Business associate contracts with subcontractors established ✓ COMPLETE

The company, as a business associate, may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic Protected Health Information (ePHI) on its behalf only if the company can obtain satisfactory assurances, in accordance with company policies, that the subcontractor will appropriately safeguard the information.

1 TEST

**Company has an approved HIPAA Compliance Policy:** Verifies that a HIPAA Compliance Policy has been created and approved within Vanta. ✓

1 DOCUMENT

**Business associate agreement template** ✓

164.308(b)(3)

Written contract or other arrangement: Document the satisfactory assurances required by paragraph (b)(1) or (b2) above of this section through a written or other arrangement with the business associate that meets the applicable requirements of 164.314(a) [the Organizational Requirements]

---

1 CONTROL

▶ **Business associate agreements documented**

✓ COMPLETE

The company documents the satisfactory assurances required for business associates and business-associated contractors through a written contract or other arrangements with the business associate that meets the applicable requirements of company policies.

1 DOCUMENT

**Business associate agreement template**

✓

---

# 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.

1 CONTROL

## ▶ Facility access controls implemented

✓ COMPLETE

The company has implemented 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.

3 TESTS

**Company has an approved Physical Security Policy:** Verifies that a Physical Security Policy has been created and approved within Vanta. ✓

**Company has an approved Third-Party Management Policy:** Verifies that a Third-Party Management Policy has been created and approved within Vanta. ✓

**Company has compliance security reports for critical vendors and reviews them annually:** Verifies that all high risk vendors on the [Vendors page](/vendors) have a completed security review in the past 12 months. ✓

1 DOCUMENT

**Vendor security review** ✓

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.

1 CONTROL

▶ Contingency operations established

✓ COMPLETE

The company has established (and implements 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.

2 TESTS

**Company has an approved Business Continuity and Disaster Recovery Plan:** Verifies that a Business Continuity and Disaster Recovery Plan has been created and approved within Vanta. ✓

**Employees agree to Business Continuity and Disaster Recovery Plan:** Verifies that all relevant employees have agreed to the Business Continuity and Disaster Recovery Plan. ✓

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.

1 CONTROL

▶ Facility security plan implemented

✓ COMPLETE

The company has implemented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

3 TESTS

**Company has an approved Physical Security Policy:** Verifies that a Physical Security Policy has been created and approved within Vanta. ✓

**Company has an approved Third-Party Management Policy:** Verifies that a Third-Party Management Policy has been created and approved within Vanta. ✓

**Company has compliance security reports for critical vendors and reviews them annually:** Verifies that all high risk vendors on the [Vendors page](/vendors) have a completed security review in the past 12 months. ✓

1 DOCUMENT

**Vendor security review** ✓

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.

---

1 CONTROL

▶ Access control and validation procedures implemented

✓ COMPLETE

The company has implemented 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.

3 TESTS

**Company has an approved Physical Security Policy:** Verifies that a Physical Security Policy has been created and approved within Vanta. ✓

**Company has an approved Third-Party Management Policy:** Verifies that a Third-Party Management Policy has been created and approved within Vanta. ✓

**Company has compliance security reports for critical vendors and reviews them annually:** Verifies that all high risk vendors on the [Vendors page](/vendors) have a completed security review in the past 12 months. ✓

1 DOCUMENT

**Vendor security review** ✓

---

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).

---

1 CONTROL

▶ Maintenance records maintained

✓ COMPLETE

The company has implemented 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).

1 TEST

**Company has an approved Physical Security Policy:** Verifies that a Physical Security Policy has been created and approved within Vanta. ✓

---

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.

---

1 CONTROL

▶ Workstation security policies implemented ✓ COMPLETE

The company has implemented policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic Protected Health Information (ePHI).

2 TESTS

**Company has an approved Asset Management Policy:** Verifies that a Asset Management Policy has been created and approved within Vanta. ✓

**Company has an approved HIPAA Workstation Security Policy:** Verifies that a HIPAA Workstation Security Policy has been created and approved within Vanta. ✓

---

164.310(c)

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

---

1 CONTROL

▶ Workstation security implemented ✓ COMPLETE

The company has implemented physical safeguards for all workstations that access electronic protected health information (ePHI), to restrict access to authorized users.

2 TESTS

**Company has an approved HIPAA Workstation Security Policy:** Verifies that a HIPAA Workstation Security Policy has been created and approved within Vanta. ✓

**Employees agree to HIPAA Workstation Security Policy:** Verifies that all relevant employees have agreed to the HIPAA Workstation Security Policy. ✓

---

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.

---

1 CONTROL

▶ Media removal policies implemented

✓ COMPLETE

The company has implemented policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic Protected Health Information (ePHI) into and out of a facility, and the movement of these items within the facility.

2 TESTS

**Company has an approved Asset Management Policy:** Verifies that a Asset Management Policy has been created and approved within Vanta.

✓

**Company has an approved Data Management Policy:** Verifies that a Data Management Policy has been created and approved within Vanta.

✓

---

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.

---

1 CONTROL

▶ Device and media disposal policies implemented

✓ COMPLETE

The company has implemented policies and procedures to address the final disposition of electronic Protected Health Information (ePHI), and/or the hardware or electronic media on which it is stored.

2 TESTS

**Company has an approved Asset Management Policy:** Verifies that a Asset Management Policy has been created and approved within Vanta.

✓

**Company has an approved Data Management Policy:** Verifies that a Data Management Policy has been created and approved within Vanta.

✓

---

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.

---

1 CONTROL

▶ Media re-use procedures implemented

✓ COMPLETE

The company has implemented procedures for removal of electronic protected health information (ePHI) from electronic media before the media are made available for re-use.

4 TESTS

**Company has an approved Asset Management Policy:** Verifies that a Asset Management Policy has been created and approved within Vanta.

✓

**Company has an approved Data Management Policy:** Verifies that a Data Management Policy has been created and approved within Vanta.

✓

**Company has an approved HIPAA Compliance Policy:** Verifies that a HIPAA Compliance Policy has been created and approved within Vanta.

✓

**Employees agree to HIPAA Compliance Policy:** Verifies that all relevant employees have agreed to the HIPAA Compliance Policy.

✓

---

164.310(d)(2)(iii)

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

---

1 CONTROL

▶ Device and media movement recorded

✓ COMPLETE

The company maintains a record of the movements of hardware and electronic media and any person responsible therefore.

2 TESTS

**Company has an approved Asset Management Policy:** Verifies that a Asset Management Policy has been created and approved within Vanta.

✓

**Company has an approved Data Management Policy:** Verifies that a Data Management Policy has been created and approved within Vanta.

✓

---

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

---

1 CONTROL

▶ Data backed up and stored

✓ COMPLETE

The company creates a retrievable, exact copy of electronic protected health information (ePHI), when needed, before the movement of equipment.

3 TESTS

**Company has an approved HIPAA Compliance Policy:** Verifies that a HIPAA Compliance Policy has been created and approved within Vanta.



**Daily database backups (Heroku):** Verifies that all Heroku databases are backed up daily. This feature is automatically provided by Heroku Postgres plans on at least the Standard tier.



**Employees agree to HIPAA Compliance Policy:** Verifies that all relevant employees have agreed to the HIPAA Compliance Policy.



# 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].

1 CONTROL

▶ Access controls applied

✓ COMPLETE

The company implements technical policies and procedures for electronic information systems that maintain electronic protected health information (ePHI) to allow access only to those persons or software programs that have been granted access rights.

1 TEST

**Company has an approved Access Control Policy:** Verifies that a Access Control Policy has been created and approved within Vanta.

✓

1 DOCUMENT

**Access request ticket and history**

✓

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.

1 CONTROL

▶ Unique user identified

✓ COMPLETE

The company assigns a unique name and/or number for identifying and tracking user identity.

6 TESTS

**Company has an approved Access Control Policy:** Verifies that a Access Control Policy has been created and approved within Vanta. ✓

**Employees have unique email accounts:** Verifies that every linked identity provider has more than one user. ✓

**Employees have unique version control accounts:** Verifies that every linked version control account has more than one user. ✓

**Service accounts used (Heroku):** This feature is built into Heroku. ✓

**No user account has a policy attached directly (Heroku):** This feature is built into Heroku. ✓

**Employees have unique SSH keys:** Verifies that any two workstations with the Vanta Agent installed share no SSH keys if the workstations are owned by different users. This test doesn't check Windows machines. ✓

164.312(a)(2)(ii)

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

1 CONTROL

▶ Emergency access procedures established

✓ COMPLETE

The company has established (and implements as needed) procedures for obtaining necessary electronic protected health information (ePHI) during an emergency.

2 TESTS

**Company has an approved Business Continuity and Disaster Recovery Plan:** Verifies that a Business Continuity and Disaster Recovery Plan has been created and approved within Vanta. ✓

**Employees agree to Business Continuity and Disaster Recovery Plan:** Verifies that all relevant employees have agreed to the Business Continuity and Disaster Recovery Plan. ✓

1 DOCUMENT

**Business associate agreement template** ✓

164.312(a)(2)(iii)

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

---

1 CONTROL

▶ Log-off automated

✓ COMPLETE

The company has implemented electronic procedures that terminate an electronic session after a predetermined time of inactivity.

2 TESTS

**Employee computer screenlock configured (MacOS):** Verifies that all employee MacOS workstations with the Vanta Agent installed have screenlock correctly configured.



**Company has an approved Access Control Policy:** Verifies that a Access Control Policy has been created and approved within Vanta.



---

164.312(a)(2)(iv)

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

---

1 CONTROL

▶ Encryption and decryption controls implemented

✓ COMPLETE

The company has implemented a mechanism to encrypt and decrypt electronic protected health information (ePHI).

7 TESTS

**Company has an approved Cryptography Policy:** Verifies that a Cryptography Policy has been created and approved within Vanta. ✓

**User data is encrypted at rest (Heroku):** Verifies that Heroku databases are encrypted at rest. This feature is automatically provided by Heroku Postgres plans on the Standard tier or higher. ✓

**Employee computer hard disk encryption:** Verifies that all employee workstations with the Vanta Agent installed have encrypted hard drives. ✓

**Strong SSL/TLS ciphers used:** Verifies that the company website (as specified on the business info page) has a valid certificate and only accepts TLS connections using up-to-date cipher suites. ✓

**SSL configuration has no known issues:** Verifies that the company website (as specified on the business info page) has a valid certificate and issues no TLS warnings. ✓



**SSL certificate has not expired:** Verifies that the company website (as specified on the business info page) has an unexpired certificate. ✓

**SSL enforced on company website:** Verifies that the company website (as specified on the business info page) redirects HTTP to HTTPS via a 3XX status code. ✓

---

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.

---

1 CONTROL

▶ **Audit controls implemented**

✓ COMPLETE

The company has implemented hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information (ePHI).

1 TEST

**User activity and API use is tracked (Heroku):** This feature is built into Heroku. ✓

---

164.312(c)(1)

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

---

1 CONTROL

▶ Data integrity maintained

✓ COMPLETE

The company has implemented policies and procedures to protect electronic protected health information (ePHI) from improper alteration or destruction.

4 TESTS

**Company has an approved Access Control Policy:** Verifies that a Access Control Policy has been created and approved within Vanta. ✓

**Company has an approved HIPAA Compliance Policy:** Verifies that a HIPAA Compliance Policy has been created and approved within Vanta. ✓

**Company has an approved Information Security Policy (AUP):** Verifies that a Information Security Policy (AUP) has been created and approved within Vanta. ✓

**Employees agree to HIPAA Compliance Policy:** Verifies that all relevant employees have agreed to the HIPAA Compliance Policy. ✓

164.312(c)(2)

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

1 CONTROL

▶ Mechanism to authenticate ePHI implemented

✓ COMPLETE

The company has implemented electronic mechanisms to corroborate that electronic protected health information (ePHI) has not been altered or destroyed in an unauthorized manner.

1 TEST

**User activity and API use is tracked (Heroku):** This feature is built into Heroku. ✓

2 DOCUMENTS

**Sample of remediated vulnerabilities** ✓

**Vulnerability scan** ✓

164.312(d)

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

## ▶ Person or entities authenticated

✓ COMPLETE

The company has implemented procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

## 4 TESTS

**Company has an approved Access Control Policy:** Verifies that a Access Control Policy has been created and approved within Vanta. ✓

**MFA on GitHub:** Verifies that MFA is enabled on all GitHub accounts that aren't marked as external or non-human. ✓

**MFA on Google Workspace:** Verifies that all members of the Google Workspace organization have multi-factor authentication enabled, unless that user has been added to the organization within the configured SLA. ✓

**MFA on Slack:** Verifies that MFA is enabled on all Slack accounts that aren't marked as external or non-human. ✓

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.

▶ Data transmission secured

✓ COMPLETE

The company has implemented technical security measures to guard against unauthorized access to electronic protected health information (ePHI) that is being transmitted over an electronic communications network.

7 TESTS

**Company has an approved Data Management Policy:** Verifies that a Data Management Policy has been created and approved within Vanta. ✓

**MFA on GitHub:** Verifies that MFA is enabled on all GitHub accounts that aren't marked as external or non-human. ✓

**MFA on Google Workspace:** Verifies that all members of the Google Workspace organization have multi-factor authentication enabled, unless that user has been added to the organization within the configured SLA. ✓

**Strong SSL/TLS ciphers used:** Verifies that the company website (as specified on the business info page) has a valid certificate and only accepts TLS connections using up-to-date cipher suites. ✓

**SSL configuration has no known issues:** Verifies that the company website (as specified on the business info page) has a valid certificate and issues no TLS warnings. ✓

**SSL certificate has not expired:** Verifies that the company website (as specified on the business info page) has an unexpired certificate. ✓

**SSL enforced on company website:** Verifies that the company website (as specified on the business info page) redirects HTTP to HTTPS via a 3XX status code. ✓

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.

1 CONTROL

▶ Data transmission integrity maintained

✓ COMPLETE

The company has implemented security measures to ensure that electronically transmitted electronic protected health information (ePHI) is not improperly modified without detection until disposed of.

6 TESTS

**Company has an approved Cryptography Policy:** Verifies that a Cryptography Policy has been created and approved within Vanta. ✓

**Company has an approved Data Management Policy:** Verifies that a Data Management Policy has been created and approved within Vanta. ✓

**Strong SSL/TLS ciphers used:** Verifies that the company website (as specified on the business info page) has a valid certificate and only accepts TLS connections using up-to-date cipher suites. ✓

**SSL configuration has no known issues:** Verifies that the company website (as specified on the business info page) has a valid certificate and issues no TLS warnings. ✓

**SSL certificate has not expired:** Verifies that the company website (as specified on the business info page) has an unexpired certificate. ✓

**SSL enforced on company website:** Verifies that the company website (as specified on the business info page) redirects HTTP to HTTPS via a 3XX status code. ✓

164.312(e)(2)(ii)

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

1 CONTROL

▶ Data transmission encrypted

✓ COMPLETE

The company has implemented a mechanism to encrypt electronic protected health information (ePHI) whenever deemed appropriate.

3 TESTS

**Company has an approved Cryptography Policy:** Verifies that a Cryptography Policy has been created and approved within Vanta. ✓

**Company has an approved Data Management Policy:** Verifies that a Data Management Policy has been created and approved within Vanta. ✓

**User data is encrypted at rest (Heroku):** Verifies that Heroku databases are encrypted at rest. This feature is automatically provided by Heroku Postgres plans on the Standard tier or higher. ✓

# 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."

## 1 CONTROL

### ▶ Business associate agreements required

 COMPLETE

The company requires an agreement contract or other arrangement from business associates that meets administrative safeguards (§ 164.308(b)(3)) and the requirements of the organization (§ 164.314(a)(2)(i), (a)(2)(ii), or (a)(2)(iii)) as applicable.

## 2 TESTS

**Company has an approved HIPAA Compliance Policy:** Verifies that a HIPAA Compliance Policy has been created and approved within Vanta. 

**Employees agree to HIPAA Compliance Policy:** Verifies that all relevant employees have agreed to the HIPAA Compliance Policy. 

## 1 DOCUMENT

**Business associate agreement template** 

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.”

---

3 CONTROLS

▶ Business associate agreements comply

✓ COMPLETE

The company requires that business associate agreements include compliance with the applicable requirements.

2 TESTS

**Company has an approved HIPAA Compliance Policy:** Verifies that a HIPAA Compliance Policy has been created and approved within Vanta.

✓

**Employees agree to HIPAA Compliance Policy:** Verifies that all relevant employees have agreed to the HIPAA Compliance Policy.

✓

1 DOCUMENT

**Business associate agreement template**

✓

---

▶ Business associate security incidents reported

✓ COMPLETE

The company requires business associates and subcontractors to report any security incident of which it becomes aware, including breaches of unsecured protected health information as required by the Breach Notification rules (§ 164.410).

1 DOCUMENT

**Business associate agreement template**

✓

---

▶ Subcontractor agreements enforced

✓ COMPLETE

The company, in accordance with administrative safeguards (§ 164.308(b)(2)), ensures that any subcontractors that create, receive, maintain, or transmit electronic Protected Health Information (ePHI) on behalf of the business associate agree to comply with the applicable requirements by entering into an agreement contract or other arrangement that complies with organization requirements.

2 TESTS

**Company has an approved HIPAA Compliance Policy:** Verifies that a HIPAA Compliance Policy has been created and approved within Vanta.

✓

**Employees agree to HIPAA Compliance Policy:** Verifies that all relevant employees have agreed to the HIPAA Compliance Policy.

✓

1 DOCUMENT

**Business associate agreement template**

✓

---

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.

## 1 CONTROL

▶ Business associate agreements with subcontractors obtained ✓ COMPLETE

The company requires that the requirements described for § 164.314(a)(2)(i) and § 164.314(a)(2)(ii) apply to the agreement contract or other arrangements between a business associate and a subcontractor in the same manner as such requirements apply to agreement contracts or other arrangements between the company and the business associate.

## 2 TESTS

**Company has an approved HIPAA Compliance Policy:** Verifies that a HIPAA Compliance Policy has been created and approved within Vanta. ✓

**Employees agree to HIPAA Compliance Policy:** Verifies that all relevant employees have agreed to the HIPAA Compliance Policy. ✓

## 1 DOCUMENT

**Business associate agreement template** ✓

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

## 1 CONTROL



▶ Group health plan information controlled

✓ COMPLETE

The company has implemented administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information (ePHI) that it creates, receives, maintains, or transmits on behalf of the group health plan.

15 TESTS

**Company has an approved Access Control Policy:** Verifies that a Access Control Policy has been created and approved within Vanta. ✓

**Company has an approved Asset Management Policy:** Verifies that a Asset Management Policy has been created and approved within Vanta. ✓

**Company has an approved Business Continuity and Disaster Recovery Plan:** Verifies that a Business Continuity and Disaster Recovery Plan has been created and approved within Vanta. ✓

**Company has an approved Cryptography Policy:** Verifies that a Cryptography Policy has been created and approved within Vanta. ✓

**Company has an approved Data Management Policy:** Verifies that a Data Management Policy has been created and approved within Vanta. ✓

**Company has an approved Human Resource Security Policy:** Verifies that a Human Resource Security Policy has been created and approved within Vanta. ✓

**Company has an approved Incident Response Plan:** Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

**Company has an approved Information Security Policy (AUP):** Verifies that a Information Security Policy (AUP) has been created and approved within Vanta. ✓

**Company has an approved Information Security Roles and Responsibilities:** Verifies that a Information Security Roles and Responsibilities has been created and approved within Vanta. ✓

**Company has an approved Operations Security Policy:** Verifies that a Operations Security Policy has been created and approved within Vanta. ✓

**Company has an approved Physical Security Policy:** Verifies that a Physical Security Policy has been created and approved within Vanta. ✓

**Company has an approved Risk Management Policy:** Verifies that a Risk Management Policy has been created and approved within Vanta. ✓

**Company has an approved Secure Development Policy:** Verifies that a Secure Development Policy has been created and approved within Vanta. ✓

**Company has an approved Third-Party Management Policy:** Verifies that a Third-Party Management Policy has been created and approved within Vanta. ✓

**Employees agree to Business Continuity and Disaster Recovery Plan:** Verifies that all relevant employees have agreed to the Business Continuity and Disaster Recovery Plan. ✓

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

---

1 CONTROL

▶ Group health plan information protected

✓ COMPLETE

The company ensures that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information.

3 TESTS

**Company has an approved HIPAA Compliance Policy:** Verifies that a HIPAA Compliance Policy has been created and approved within Vanta. ✓

**Employees agree to HIPAA Compliance Policy:** Verifies that all relevant employees have agreed to the HIPAA Compliance Policy. ✓

**Company has compliance security reports for critical vendors and reviews them annually:** Verifies that all high risk vendors on the [Vendors page](/vendors) have a completed security review in the past 12 months. ✓

1 DOCUMENT

**Business associate agreement template** ✓

---

164.314(b)(2)(iv)

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

---

1 CONTROL

▶ Group health plan security incidents reported

✓ COMPLETE

The company reports to the group health plan any security incident of which it becomes aware.

2 TESTS

**Company has an approved Incident Response Plan:** Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

**Company has an approved Incident Response Plan HIPAA Addendum with Breach Notification Procedures:** Verifies that a Incident Response Plan HIPAA Addendum with Breach Notification Procedures has been created and approved within Vanta. ✓

---

# 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.

---

1 CONTROL

► Policies and procedures created

✓ COMPLETE

The company, as a covered entity or business associate, must, in accordance with the HIPAA security rule (§ 164.306), implement reasonable and appropriate policies and procedures to comply with implementation specifications, or other requirements, taking into account those factors specified in the HIPAA security general rules (§ 164.306(b)(2)(i), (ii), (iii), and (iv)).

This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements (§164.316).

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.

18 TESTS

**Company has an approved Access Control Policy:** Verifies that a Access Control Policy has been created and approved within Vanta. ✓

**Company has an approved Asset Management Policy:** Verifies that a Asset Management Policy has been created and approved within Vanta. ✓

**Company has an approved Business Continuity and Disaster Recovery Plan:** Verifies that a Business Continuity and Disaster Recovery Plan has been created and approved within Vanta. ✓

**Company has an approved Cryptography Policy:** Verifies that a Cryptography Policy has been created and approved within Vanta. ✓

**Company has an approved Data Management Policy:** Verifies that a Data Management Policy has been created and approved within Vanta. ✓

**Company has an approved HIPAA Compliance Policy:** Verifies that a HIPAA Compliance Policy has been created and approved within Vanta. ✓

**Company has an approved Human Resource Security Policy:** Verifies that a Human Resource Security Policy has been created and approved within Vanta. ✓

**Company has an approved Incident Response Plan:** Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

**Company has an approved Incident Response Plan HIPAA Addendum with Breach Notification Procedures:** Verifies that a Incident Response Plan HIPAA Addendum with Breach Notification Procedures has been created and approved within Vanta. ✓

**Company has an approved Information Security Policy (AUP):** Verifies that a Information Security Policy (AUP) has been created and approved within Vanta. ✓

**Company has an approved Information Security Roles and Responsibilities:** Verifies that a Information Security Roles and Responsibilities has been created and approved within Vanta. ✓

**Company has an approved Operations Security Policy:** Verifies that a Operations Security Policy has been created and approved within Vanta. ✓

**Company has an approved Physical Security Policy:** Verifies that a Physical Security Policy has been created and approved within Vanta. ✓

**Company has an approved Risk Management Policy:** Verifies that a Risk Management Policy has been created and approved within Vanta. ✓

- Company has an approved Secure Development Policy:** Verifies that a Secure Development Policy has been created and approved within Vanta. ✓
  - Company has an approved Third-Party Management Policy:** Verifies that a Third-Party Management Policy has been created and approved within Vanta. ✓
  - Employees agree to Business Continuity and Disaster Recovery Plan:** Verifies that all relevant employees have agreed to the Business Continuity and Disaster Recovery Plan. ✓
  - Employees agree to HIPAA Compliance Policy:** Verifies that all relevant employees have agreed to the HIPAA Compliance Policy. ✓
- 

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.

---

1 CONTROL

► Policies and procedures documented

✓ COMPLETE

The company maintains the policies and procedures implemented to comply with the HIPAA security safeguards in written (which may be electronic) form.

18 TESTS

**Company has an approved Access Control Policy:** Verifies that a Access Control Policy has been created and approved within Vanta. ✓

**Company has an approved Asset Management Policy:** Verifies that a Asset Management Policy has been created and approved within Vanta. ✓

**Company has an approved Business Continuity and Disaster Recovery Plan:** Verifies that a Business Continuity and Disaster Recovery Plan has been created and approved within Vanta. ✓

**Company has an approved Cryptography Policy:** Verifies that a Cryptography Policy has been created and approved within Vanta. ✓

**Company has an approved Data Management Policy:** Verifies that a Data Management Policy has been created and approved within Vanta. ✓

**Company has an approved HIPAA Compliance Policy:** Verifies that a HIPAA Compliance Policy has been created and approved within Vanta. ✓

**Company has an approved Human Resource Security Policy:** Verifies that a Human Resource Security Policy has been created and approved within Vanta. ✓

**Company has an approved Incident Response Plan:** Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

**Company has an approved Incident Response Plan HIPAA Addendum with Breach Notification Procedures:** Verifies that a Incident Response Plan HIPAA Addendum with Breach Notification Procedures has been created and approved within Vanta. ✓

**Company has an approved Information Security Policy (AUP):** Verifies that a Information Security Policy (AUP) has been created and approved within Vanta. ✓

**Company has an approved Information Security Roles and Responsibilities:** Verifies that a Information Security Roles and Responsibilities has been created and approved within Vanta. ✓

**Company has an approved Operations Security Policy:** Verifies that a Operations Security Policy has been created and approved within Vanta. ✓

**Company has an approved Physical Security Policy:** Verifies that a Physical Security Policy has been created and approved within Vanta. ✓

**Company has an approved Risk Management Policy:** Verifies that a Risk Management Policy has been created and approved within Vanta. ✓

**Company has an approved Secure Development Policy:** Verifies that a Secure Development Policy has been created and approved within Vanta. ✓

**Company has an approved Third-Party Management Policy:** Verifies that a Third-Party Management Policy has been created and approved within Vanta. ✓

**Employees agree to Business Continuity and Disaster Recovery Plan:** Verifies that all relevant employees have agreed to the Business Continuity and Disaster Recovery Plan. ✓

**Employees agree to HIPAA Compliance Policy:** Verifies that all relevant employees have agreed to the HIPAA Compliance Policy.



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.

1 CONTROL

► Policies and procedures activity documented

✓ COMPLETE

Where an action, activity or assessment is required (described in § 164.316) to be documented, the company maintains a written (which may be electronic) record of the action, activity, or assessment.

6 TESTS

**Company has an approved Access Control Policy:** Verifies that a Access Control Policy has been created and approved within Vanta.



**Company has an approved Data Management Policy:** Verifies that a Data Management Policy has been created and approved within Vanta.



**Company has an approved HIPAA Compliance Policy:** Verifies that a HIPAA Compliance Policy has been created and approved within Vanta.



**Company has an approved Information Security Policy (AUP):** Verifies that a Information Security Policy (AUP) has been created and approved within Vanta.



**Employees agree to HIPAA Compliance Policy:** Verifies that all relevant employees have agreed to the HIPAA Compliance Policy.



**HIPAA risks are reviewed annually:** Verifies that at least one Privacy-related risk is included in a valid snapshot of the risk register (i.e. a snapshot taken in the past year)



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.

1 CONTROL

▶ Data retention and time limit

✓ COMPLETE

The company retains the documentation of policies, procedures and action, activity or assessments as required by paragraph 316(b)(1) of the HIPAA rules for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

2 TESTS

**Company has an approved HIPAA Compliance Policy:** Verifies that a HIPAA Compliance Policy has been created and approved within Vanta.



**Employees agree to HIPAA Compliance Policy:** Verifies that all relevant employees have agreed to the HIPAA Compliance Policy.



164.316(b)(2)(ii)

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

1 CONTROL



► Policies and procedures available

✓ COMPLETE

The company makes documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

32 TESTS

**Company has an approved Access Control Policy:** Verifies that a Access Control Policy has been created and approved within Vanta. ✓

**Company has an approved Asset Management Policy:** Verifies that a Asset Management Policy has been created and approved within Vanta. ✓

**Company has an approved Business Continuity and Disaster Recovery Plan:** Verifies that a Business Continuity and Disaster Recovery Plan has been created and approved within Vanta. ✓

**Company has an approved Cryptography Policy:** Verifies that a Cryptography Policy has been created and approved within Vanta. ✓

**Company has an approved Data Management Policy:** Verifies that a Data Management Policy has been created and approved within Vanta. ✓

**Company has an approved HIPAA Compliance Policy:** Verifies that a HIPAA Compliance Policy has been created and approved within Vanta. ✓

**Company has an approved Human Resource Security Policy:** Verifies that a Human Resource Security Policy has been created and approved within Vanta. ✓

**Company has an approved Incident Response Plan:** Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

**Company has an approved Incident Response Plan HIPAA Addendum with Breach Notification Procedures:** Verifies that a Incident Response Plan HIPAA Addendum with Breach Notification Procedures has been created and approved within Vanta. ✓

**Company has an approved Information Security Policy (AUP):** Verifies that a Information Security Policy (AUP) has been created and approved within Vanta. ✓

**Company has an approved Information Security Roles and Responsibilities:** Verifies that a Information Security Roles and Responsibilities has been created and approved within Vanta. ✓

**Company has an approved Operations Security Policy:** Verifies that a Operations Security Policy has been created and approved within Vanta. ✓

**Company has an approved Physical Security Policy:** Verifies that a Physical Security Policy has been created and approved within Vanta. ✓

**Company has an approved Risk Management Policy:** Verifies that a Risk Management Policy has been created and approved within Vanta. ✓

**Company has an approved Secure Development Policy:** Verifies that a Secure Development Policy has been created and approved within Vanta. ✓

**Company has an approved Third-Party Management Policy:** Verifies that a Third-Party Management Policy has been created and approved within Vanta. ✓

**Employees agree to Access Control Policy:** Verifies that all relevant employees have agreed to the Access Control Policy. ✓

- Employees agree to Asset Management Policy:** Verifies that all relevant employees have agreed to the Asset Management Policy. ✓
- Employees agree to Business Continuity and Disaster Recovery Plan:** Verifies that all relevant employees have agreed to the Business Continuity and Disaster Recovery Plan. ✓
- Employees agree to Code of Conduct:** Verifies that all relevant employees have agreed to the Code of Conduct. ✓
- Employees agree to Cryptography Policy:** Verifies that all relevant employees have agreed to the Cryptography Policy. ✓
- Employees agree to Data Management Policy:** Verifies that all relevant employees have agreed to the Data Management Policy. ✓
- Employees agree to HIPAA Compliance Policy:** Verifies that all relevant employees have agreed to the HIPAA Compliance Policy. ✓
- Employees agree to Human Resource Security Policy:** Verifies that all relevant employees have agreed to the Human Resource Security Policy. ✓
- Employees agree to Incident Response Plan:** Verifies that all relevant employees have agreed to the Incident Response Plan. ✓
- Employees agree to Information Security Policy (AUP):** Verifies that all relevant employees have agreed to the Information Security Policy (AUP). ✓
- Employees agree to Information Security Roles and Responsibilities:** Verifies that all relevant employees have agreed to the Information Security Roles and Responsibilities. ✓
- Employees agree to Operations Security Policy:** Verifies that all relevant employees have agreed to the Operations Security Policy. ✓
- Employees agree to Physical Security Policy:** Verifies that all relevant employees have agreed to the Physical Security Policy. ✓
- Employees agree to Risk Management Policy:** Verifies that all relevant employees have agreed to the Risk Management Policy. ✓
- Employees agree to Secure Development Policy:** Verifies that all relevant employees have agreed to the Secure Development Policy. ✓
- Employees agree to Third-Party Management Policy:** Verifies that all relevant employees have agreed to the Third-Party Management Policy. ✓

1 DOCUMENT

- Publicly available privacy policy** ✓

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.

1 CONTROL

▶ Policies and procedures updated

✓ COMPLETE

The company reviews documentation periodically, and updates as needed, in response to environmental or operational changes affecting the security of electronic protected health information (ePHI).

3 TESTS

**Company has an approved HIPAA Compliance Policy:** Verifies that a HIPAA Compliance Policy has been created and approved within Vanta.



**Company has an approved Incident Response Plan HIPAA Addendum with Breach Notification Procedures:** Verifies that a Incident Response Plan HIPAA Addendum with Breach Notification Procedures has been created and approved within Vanta.



**Employees agree to HIPAA Compliance Policy:** Verifies that all relevant employees have agreed to the HIPAA Compliance Policy.



## Notification to individuals

164.404 (2)

For purposes of paragraph (a)(1) of this section, §§ 164.406(a), and 164.408(a), a breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).

### 1 CONTROL


#### ▶ Additional breach information

 COMPLETE

A business associate provides the company, as a covered entity, with any other available information that the company is required to include in notification to the individual (described in 164.404(c)) at the time of the notification or promptly thereafter as information becomes available.

### 2 TESTS

**Company has an approved Incident Response Plan:** Verifies that a Incident Response Plan has been created and approved within Vanta. 

**Company has an approved Incident Response Plan HIPAA Addendum with Breach Notification Procedures:** Verifies that a Incident Response Plan HIPAA Addendum with Breach Notification Procedures has been created and approved within Vanta. 

164.404(a)

A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used or disclosed as a result of such breach.

### 1 CONTROL

▶ Additional breach information

✓ COMPLETE

A business associate provides the company, as a covered entity, with any other available information that the company is required to include in notification to the individual (described in 164.404(c)) at the time of the notification or promptly thereafter as information becomes available.

2 TESTS

**Company has an approved Incident Response Plan:** Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

**Company has an approved Incident Response Plan HIPAA Addendum with Breach Notification Procedures:** Verifies that a Incident Response Plan HIPAA Addendum with Breach Notification Procedures has been created and approved within Vanta. ✓

164.404(b)

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

1 CONTROL

▶ Additional breach information

✓ COMPLETE

A business associate provides the company, as a covered entity, with any other available information that the company is required to include in notification to the individual (described in 164.404(c)) at the time of the notification or promptly thereafter as information becomes available.

2 TESTS

**Company has an approved Incident Response Plan:** Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

**Company has an approved Incident Response Plan HIPAA Addendum with Breach Notification Procedures:** Verifies that a Incident Response Plan HIPAA Addendum with Breach Notification Procedures has been created and approved within Vanta. ✓

164.404(c)(1)

Elements of the notification required by paragraph (a) of this section shall include to the extent possible: (A) a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known; (B) a description of the types of unsecured protected health information that were involved in the breach (Such as whether full name, social security number, date of birth, home address,

account number, diagnosis, disability code, or other types of information were involved); (C) any steps the individual should take to protect themselves from potential harm resulting from the breach; (D) a brief description of what the covered entity is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches; and (E) contact procedures for individuals to ask questions or learn additional information which should include a toll-free number, an email address, website, or postal address.

---

1 CONTROL

▶ Additional breach information

✓ COMPLETE

A business associate provides the company, as a covered entity, with any other available information that the company is required to include in notification to the individual (described in 164.404(c)) at the time of the notification or promptly thereafter as information becomes available.

2 TESTS

**Company has an approved Incident Response Plan:** Verifies that a Incident Response Plan has been created and approved within Vanta.



**Company has an approved Incident Response Plan HIPAA Addendum with Breach Notification Procedures:** Verifies that a Incident Response Plan HIPAA Addendum with Breach Notification Procedures has been created and approved within Vanta.



164.404(c)(2)

The notification required by paragraph (a) of this section shall be written in plain language.

---

1 CONTROL

▶ Additional breach information

✓ COMPLETE

A business associate provides the company, as a covered entity, with any other available information that the company is required to include in notification to the individual (described in 164.404(c)) at the time of the notification or promptly thereafter as information becomes available.

2 TESTS

**Company has an approved Incident Response Plan:** Verifies that a Incident Response Plan has been created and approved within Vanta.



**Company has an approved Incident Response Plan HIPAA Addendum with Breach Notification Procedures:** Verifies that a Incident Response Plan HIPAA Addendum with Breach Notification Procedures has been created and approved within Vanta.



The notification required by paragraph (a) shall be provided in the following form: Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as more information becomes available.

## 1 CONTROL

▶ Additional breach information

✓ COMPLETE

A business associate provides the company, as a covered entity, with any other available information that the company is required to include in notification to the individual (described in 164.404(c)) at the time of the notification or promptly thereafter as information becomes available.

## 2 TESTS

**Company has an approved Incident Response Plan:** Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

**Company has an approved Incident Response Plan HIPAA Addendum with Breach Notification Procedures:** Verifies that a Incident Response Plan HIPAA Addendum with Breach Notification Procedures has been created and approved within Vanta. ✓

The notification required by paragraph (a) shall be provided in the following form: If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual (as specified under §164.502(g)(4) of subpart E) , written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available.

## 1 CONTROL

▶ Additional breach information

✓ COMPLETE

A business associate provides the company, as a covered entity, with any other available information that the company is required to include in notification to the individual (described in 164.404(c)) at the time of the notification or promptly thereafter as information becomes available.

2 TESTS

**Company has an approved Incident Response Plan:** Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

**Company has an approved Incident Response Plan HIPAA Addendum with Breach Notification Procedures:** Verifies that a Incident Response Plan HIPAA Addendum with Breach Notification Procedures has been created and approved within Vanta. ✓

164.404(d)(2)

Substitute notice. In the case where there is insufficient or out-of-date contact information that precludes written notification to the individual under this paragraph (d)(1)(i) of this section, a substitute form of notice reasonable calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual under paragraph (d)(1)(ii).

1 CONTROL

▶ Additional breach information

✓ COMPLETE

A business associate provides the company, as a covered entity, with any other available information that the company is required to include in notification to the individual (described in 164.404(c)) at the time of the notification or promptly thereafter as information becomes available.

2 TESTS

**Company has an approved Incident Response Plan:** Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

**Company has an approved Incident Response Plan HIPAA Addendum with Breach Notification Procedures:** Verifies that a Incident Response Plan HIPAA Addendum with Breach Notification Procedures has been created and approved within Vanta. ✓

164.404(d)(2)(i)

In the case where there is insufficient or out-of-date contact information for fewer than 10 individuals, then substitute notice may be provided by



an alternative form of written notice, telephone or other means.

---

1 CONTROL

▶ Additional breach information

✓ COMPLETE

A business associate provides the company, as a covered entity, with any other available information that the company is required to include in notification to the individual (described in 164.404(c)) at the time of the notification or promptly thereafter as information becomes available.

2 TESTS

**Company has an approved Incident Response Plan:** Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

**Company has an approved Incident Response Plan HIPAA Addendum with Breach Notification Procedures:** Verifies that a Incident Response Plan HIPAA Addendum with Breach Notification Procedures has been created and approved within Vanta. ✓

---

164.404(d)(2)(ii)

In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall: (A) be in the form of either a conspicuous posting for a period of 90 days on the home page of the web site of the covered entity involved, or conspicuous notice in a major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and (B) include a toll-free number that remains active for at least 90 days where an individual can learn whether the individual's secured protected health information may be included in the breach.

---

1 CONTROL

▶ Additional breach information

✓ COMPLETE

A business associate provides the company, as a covered entity, with any other available information that the company is required to include in notification to the individual (described in 164.404(c)) at the time of the notification or promptly thereafter as information becomes available.

2 TESTS

**Company has an approved Incident Response Plan:** Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

**Company has an approved Incident Response Plan HIPAA Addendum with Breach Notification Procedures:** Verifies that a Incident Response Plan HIPAA Addendum with Breach Notification Procedures has been created and approved within Vanta. ✓

---

In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under paragraph (d)(1) of this section.

---

1 CONTROL

▶ Additional breach information

✓ COMPLETE

A business associate provides the company, as a covered entity, with any other available information that the company is required to include in notification to the individual (described in 164.404(c)) at the time of the notification or promptly thereafter as information becomes available.

2 TESTS

**Company has an approved Incident Response Plan:** Verifies that a Incident Response Plan has been created and approved within Vanta.

✓

**Company has an approved Incident Response Plan HIPAA Addendum with Breach Notification Procedures:** Verifies that a Incident Response Plan HIPAA Addendum with Breach Notification Procedures has been created and approved within Vanta.

✓

---

# Notification to the media

164.406(a)

For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach, notify prominent media outlets serving the State or jurisdiction

1 CONTROL

▶ Additional breach information

✓ COMPLETE

A business associate provides the company, as a covered entity, with any other available information that the company is required to include in notification to the individual (described in 164.404(c)) at the time of the notification or promptly thereafter as information becomes available.

2 TESTS

**Company has an approved Incident Response Plan:** Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

**Company has an approved Incident Response Plan HIPAA Addendum with Breach Notification Procedures:** Verifies that a Incident Response Plan HIPAA Addendum with Breach Notification Procedures has been created and approved within Vanta. ✓

164.406(b)

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

1 CONTROL

▶ Additional breach information

✓ COMPLETE

A business associate provides the company, as a covered entity, with any other available information that the company is required to include in notification to the individual (described in 164.404(c)) at the time of the notification or promptly thereafter as information becomes available.

2 TESTS

**Company has an approved Incident Response Plan:** Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

**Company has an approved Incident Response Plan HIPAA Addendum with Breach Notification Procedures:** Verifies that a Incident Response Plan HIPAA Addendum with Breach Notification Procedures has been created and approved within Vanta. ✓

164.406(c)

The content of the notification required by paragraph (a) shall meet the requirements of §164.404(c)

1 CONTROL

▶ Additional breach information

✓ COMPLETE

A business associate provides the company, as a covered entity, with any other available information that the company is required to include in notification to the individual (described in 164.404(c)) at the time of the notification or promptly thereafter as information becomes available.

2 TESTS

**Company has an approved Incident Response Plan:** Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

**Company has an approved Incident Response Plan HIPAA Addendum with Breach Notification Procedures:** Verifies that a Incident Response Plan HIPAA Addendum with Breach Notification Procedures has been created and approved within Vanta. ✓

# Notification to the Secretary.

164.408(a)

A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in §164.404(a)(2), notify the Secretary.

1 CONTROL

▶ Additional breach information

✓ COMPLETE

A business associate provides the company, as a covered entity, with any other available information that the company is required to include in notification to the individual (described in 164.404(c)) at the time of the notification or promptly thereafter as information becomes available.

2 TESTS

**Company has an approved Incident Response Plan:** Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

**Company has an approved Incident Response Plan HIPAA Addendum with Breach Notification Procedures:** Verifies that a Incident Response Plan HIPAA Addendum with Breach Notification Procedures has been created and approved within Vanta. ✓

164.408(b)

For breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall, except as provided in §164.412, provide the notification required by paragraph (a) contemporaneously with the notice required by §164.404(a) and in the manner specified on the HHS web site.

1 CONTROL

▶ Additional breach information

✓ COMPLETE

A business associate provides the company, as a covered entity, with any other available information that the company is required to include in notification to the individual (described in 164.404(c)) at the time of the notification or promptly thereafter as information becomes available.

2 TESTS

**Company has an approved Incident Response Plan:** Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

**Company has an approved Incident Response Plan HIPAA Addendum with Breach Notification Procedures:** Verifies that a Incident Response Plan HIPAA Addendum with Breach Notification Procedures has been created and approved within Vanta. ✓

164.408(c)

For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches occurring during the preceding calendar year, in a manner specified on the HHS web site.

1 CONTROL

▶ Additional breach information

✓ COMPLETE

A business associate provides the company, as a covered entity, with any other available information that the company is required to include in notification to the individual (described in 164.404(c)) at the time of the notification or promptly thereafter as information becomes available.

2 TESTS

**Company has an approved Incident Response Plan:** Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

**Company has an approved Incident Response Plan HIPAA Addendum with Breach Notification Procedures:** Verifies that a Incident Response Plan HIPAA Addendum with Breach Notification Procedures has been created and approved within Vanta. ✓

# 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.

## 1 CONTROL

### ▶ Notification of breach


 COMPLETE

The company, as a covered entity, requires all business associates, following the discovery of a breach of unsecured protected health information, to notify the company of such breach.

A breach is 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 due diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agents of the business associate (determined in accordance with the Federal common law of agency).

## 2 TESTS

**Company has an approved Incident Response Plan:** Verifies that a Incident Response Plan has been created and approved within Vanta. 

**Company has an approved Incident Response Plan HIPAA Addendum with Breach Notification Procedures:** Verifies that a Incident Response Plan HIPAA Addendum with Breach Notification Procedures has been created and approved within Vanta. 

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).

---

1 CONTROL

► Notification of breach

✓ COMPLETE

The company, as a covered entity, requires all business associates, following the discovery of a breach of unsecured protected health information, to notify the company of such breach.

A breach is 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 due diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agents of the business associate (determined in accordance with the Federal common law of agency).

2 TESTS

**Company has an approved Incident Response Plan:** Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

**Company has an approved Incident Response Plan HIPAA Addendum with Breach Notification Procedures:** Verifies that a Incident Response Plan HIPAA Addendum with Breach Notification Procedures has been created and approved within Vanta. ✓

---

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.

---

1 CONTROL



▶ Timeliness of breach notification

✓ COMPLETE

Except in cases of a law enforcement delay ( § 164.412), a business associate provides the breach notification required by the company Breach Notification policy ( § 164.410(a)) without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach.

3 TESTS

**Company has an approved Incident Response Plan:** Verifies that a Incident Response Plan has been created and approved within Vanta.



**Company has an approved Incident Response Plan HIPAA Addendum with Breach Notification Procedures:** Verifies that a Incident Response Plan HIPAA Addendum with Breach Notification Procedures has been created and approved within Vanta. ✓

**Employees agree to Incident Response Plan HIPAA Addendum with Breach Notification Procedures:** Verifies that all relevant employees have agreed to the Incident Response Plan HIPAA Addendum with Breach Notification Procedures. ✓

---

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.

---

1 CONTROL

▶ Breach notice identification of individuals

✓ COMPLETE

A business associate's breach notification includes, 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 disclosed during the breach.

2 TESTS

**Company has an approved Incident Response Plan:** Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

**Company has an approved Incident Response Plan HIPAA Addendum with Breach Notification Procedures:** Verifies that a Incident Response Plan HIPAA Addendum with Breach Notification Procedures has been created and approved within Vanta. ✓

---

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.

---

1 CONTROL

## ▶ Additional breach information

✓ COMPLETE

A business associate provides the company, as a covered entity, with any other available information that the company is required to include in notification to the individual (described in 164.404(c)) at the time of the notification or promptly thereafter as information becomes available.

2 TESTS

**Company has an approved Incident Response Plan:** Verifies that a Incident Response Plan has been created and approved within Vanta. ✓

**Company has an approved Incident Response Plan HIPAA Addendum with Breach Notification Procedures:** Verifies that a Incident Response Plan HIPAA Addendum with Breach Notification Procedures has been created and approved within Vanta. ✓

## Appendix A: Definitions

**Bug bounty program:** A crowdsourcing initiative that rewards individuals for discovering and reporting software bugs, especially those that could cause security vulnerabilities or breaches.

**DDoS:** Distributed denial of service. A DDoS attack is attack in which multiple compromised computer systems flood a target—such as a server, website, or other network resource—with messages or requests to cause a denial of service for users of the targeted resource.

**Multifactor authentication (MFA):** A security system that requires multiple methods of authentication using different types of credentials to verify users' identities before they can access a service.

**Penetration test:** The practice of testing a computer system, network, or web application to find vulnerabilities that an attacker might exploit.

**Principle of least privilege:** The principle of giving a user or account only the privileges that are required to perform a job or necessary function.

**Protected data:** Data that is protected from public view or use; includes personally identifiable information, sensitive data, HIPAA data, or financial data.

**Sensitive data:** Any information a reasonable person considers private or would choose not to share with the public.

**SSH:** Secure shell. A cryptographic network protocol for operating network services securely over an unsecured network.

**SSL:** Secure sockets layer. The standard security technology for establishing an encrypted link between a web server and a browser.

# Appendix B: Document history

Vanta continuously monitors the company's security and IT infrastructure to ensure the company complies with industry-standard security standards. Vanta tests the company's security posture continuously, and this report is automatically updated to reflect the latest findings.

## About Vanta

[Vanta](#) provides a set of security and compliance tools that scan, verify, and secure a company's IT systems and processes. Our cloud-based technology identifies security flaws and privacy gaps in a company's security posture, providing a comprehensive view across cloud infrastructure, endpoints, corporate procedures, enterprise risk, and employee accounts.

Vanta is based in San Francisco, California.

