

HIPAA SECURITY RULE ASSESSMENT

Sample Dental Group (made up) · Covered entity · Report date Oct 16, 2026

70/70 ITEMS ASSESSED	39 IN PLACE	19 PARTLY	4 NOT IN PLACE	22/22 ADDRESSABLE DECISIONS DOCUMENTED	4 HIGH OR VERY HIGH RISKS
-------------------------	----------------	--------------	-------------------	---	------------------------------

This assessment supports the client's risk analysis under 45 CFR 164.308(a)(1)(ii)(A) and the documentation the Security Rule requires (164.316). It records what was found on the dates given. It is not legal advice, an audit, an investigation or determination by the HHS Office for Civil Rights, or a certification of any kind, and it does not cover the HIPAA Privacy or Breach Notification Rules.

SCOPE

Client	Sample Dental Group (made up)
Entity	Covered entity, Dental practice, 14 staff, one office
Security official	J. Example, practice administrator
Assessor	Alex Example, Example Security Partners
Assessment dates	Oct 5, 2026 to Oct 16, 2026
Systems with ePHI in scope	Practice management and charting system (cloud, run by the vendor) Digital X-ray imaging server (in the office server closet) Microsoft 365 email and files Online appointment-reminder service (patient names and phone numbers) 6 laptops and 16 workstations and servers managed by the IT provider
Scope notes	The one office and its systems above. The billing service's own systems are out of scope (covered by its business associate agreement).

The assessment covered 22 standards and 48 implementation specifications (26 required, 22 addressable) across the administrative, physical, technical and organizational safeguards and the policies and documentation requirements. Each was rated In place, Partly, Not in place or Not applicable from interviews and the evidence listed, with NIST SP 800-66 Rev. 2's key activities and sample questions as the guide. Gaps were rated for likelihood and impact with the client.

SUMMARY BY SAFEGUARD

Safeguard	Items	In place	Partly	Not in place	N/A	Not assessed	Gaps
Administrative (164.308)	30	16	11	2	1	0	13
Physical (164.310)	12	8	3	1	0	0	3
Technical (164.312)	12	8	3	1	0	0	4
Organizational (164.314)	11	3	1	0	7	0	1
Policies and documentation (164.316)	5	4	1	0	0	0	1

GAPS

Administrative Safeguards (164.308)

Ref	Item	Status	Finding
164.308(a)(1)(ii)(D)	Information System Activity Review (R)	Not in place	Nobody reviews the charting system's access report or Microsoft 365 sign-in activity.
164.308(a)(1)(ii)(A)	Risk Analysis (R)	Partly	The last risk analysis is from 2023, by the previous IT provider. It does not cover the cloud charting system adopted in 2025, the replacement imaging server or Microsoft 365. This assessment is the update.
164.308(a)(7)(ii)(C)	Emergency Mode Operation Plan (R)	Not in place	No procedure for seeing patients while the charting system is down.
164.308(b)(3)	Written Contract or Other Arrangement (R)	Partly	No business associate agreement for the online appointment-reminder service, which receives patient names and phone numbers.
164.308(a)(4)(ii)(B)	Access Authorization (A)	Partly	The front-desk role can read clinical notes, which it does not need.
164.308(a)(6)(ii)	Response and Reporting (R)	Partly	The Oct 13, 2026 email fraud was handled and documented, but the incident response plan is a September draft, not approved, and has never been exercised.
164.308(a)(1)(ii)(B)	Risk Management (R)	Partly	No risk register. Fixes are tracked only as tickets with the IT provider.
164.308(a)(4)(ii)(C)	Access Establishment and Modification (A)	Partly	Access changes are made on request, but nobody reviews who has access.
164.308(a)(7)(ii)(B)	Disaster Recovery Plan (R)	Partly	The imaging server was restored in a test on Oct 7 (2 hours 40 minutes). Nothing is written for an outage at the charting vendor or the loss of the office network.
164.308(a)(7)	Contingency Plan (standard)	Partly	Backups and a restore test exist, but there is no single contingency plan.
164.308(a)(8)	Evaluation (standard)	Partly	No evaluation between 2023 and this assessment.
164.308(a)(3)(ii)(B)	Workforce Clearance Procedure (A)	Partly	Front-desk temps from the staffing agency start before their access is reviewed, and the agency's checks are not confirmed.
164.308(a)(7)(ii)(D)	Testing and Revision Procedures (A)	Partly	Restore tested Oct 7; the plan itself has not been tested.

Physical Safeguards (164.310)

Ref	Item	Status	Finding
164.310(a)(2)(iii)	Access Control and Validation Procedures (A)	Partly	IT provider technicians and the imaging vendor's engineer are not signed in.
164.310(d)(2)(iii)	Accountability (A)	Partly	The asset list was last updated in November 2025; two replaced workstations are missing from it.
164.310(c)	Workstation Security (standard)	Partly	The two front-desk screens face the waiting room and have no privacy filters.

Technical Safeguards (164.312)

Ref	Item	Status	Finding
164.312(d)	Person or Entity Authentication (standard)	Partly	MFA on every mailbox and the VPN since Oct 14, 2026. The IT provider's remote-support tool has no MFA.
164.312(b)	Audit Controls (standard)	Not in place	The charting system keeps audit logs, but Microsoft 365 audit logs stay only 90 days and no logs are collected or monitored.
164.312(e)(2)(ii)	Encryption (A)	Partly	Email to patients and labs is encrypted only when staff add the [secure] tag. DMARC is set to p=none.
164.312(a)(2)(i)	Unique User Identification (R)	Partly	Two shared logins, on the sterilization-room and X-ray workstations.

Organizational Requirements (164.314)

Ref	Item	Status	Finding
164.314(a)(2)(i)(A)	Business Associate Contracts: Comply with the Security Rule (R)	Partly	The imaging vendor's 2012 agreement does not require it to comply with the Security Rule.

Policies and Procedures and Documentation Requirements (164.316)

Ref	Item	Status	Finding
164.316(b)(2)(i)	Time Limit (R)	Partly	Older policies were thrown away when the 2026 set was approved.

ADDRESSABLE SPECIFICATIONS: DECISIONS

For each addressable specification the rule requires the client to assess whether it is reasonable and appropriate, then implement it, implement an equivalent alternative measure, or document why neither is reasonable and appropriate. Missing reasons are marked.

Ref	Specification	Status	Decision	Documented reason
164.308(a)(3)(ii)(A)	Authorization and/or Supervision	In place	Implemented	All staff work on site under the office manager or a dentist; for a 14-person practice, supervision is reasonable and appropriate.
164.308(a)(3)(ii)(B)	Workforce Clearance Procedure	Partly	Implemented	Background checks before access are reasonable and appropriate for every workforce member.
164.308(a)(3)(ii)(C)	Termination Procedures	In place	Implemented	A leaver checklist covers the charting system, Microsoft 365, the VPN and building fobs.
164.308(a)(4)(ii)(B)	Access Authorization	Partly	Implemented	The charting system supports roles, so role-based authorization is reasonable and appropriate.
164.308(a)(4)(ii)(C)	Access Establishment and Modification	Partly	Implemented	Changes go to the IT provider in writing; a periodic review is reasonable and appropriate.
164.308(a)(5)(ii)(A)	Security Reminders	In place	Implemented	A monthly reminder at the staff meeting, and an email after the Oct 13 payment fraud.
164.308(a)(5)(ii)(B)	Protection from Malicious Software	In place	Implemented	EDR on all 22 computers and servers; training covers reporting suspicious attachments.

Ref	Specification	Status	Decision	Documented reason
164.308(a)(5)(ii)(C)	Log-in Monitoring	In place	Alternative measure	Rather than train staff to watch log-in attempts, the IT provider's EDR and Microsoft 365 alerts flag failed and risky sign-ins to the IT provider. Staff are trained to report lockouts and unexpected MFA prompts.
164.308(a)(5)(ii)(D)	Password Management	In place	Implemented	Password manager for the few shared vendor accounts; MFA on every mailbox since Oct 14, 2026.
164.308(a)(7)(ii)(D)	Testing and Revision Procedures	Partly	Implemented	A yearly restore test and a yearly tabletop are reasonable and appropriate.
164.308(a)(7)(ii)(E)	Applications and Data Criticality Analysis	In place	Implemented	The charting system, imaging and Microsoft 365 are ranked in the backup plan, Sep 2026.
164.310(a)(2)(i)	Contingency Operations	In place	Implemented	The managing dentist and practice administrator hold keys and alarm codes for after-hours restoration.
164.310(a)(2)(ii)	Facility Security Plan	In place	Implemented	Alarm, locked server closet, and the front door is staffed during hours.
164.310(a)(2)(iii)	Access Control and Validation Procedures	Partly	Implemented	Staff fobs and a visitor sign-in are reasonable and appropriate.
164.310(a)(2)(iv)	Maintenance Records	Not in place	Not reasonable and appropriate	The practice leases one suite. The landlord maintains the building and keeps repair records for its doors, walls and locks; a separate log at the practice would add nothing. Equivalent measure: the practice asks the landlord for the records each year, and server-closet lock changes are logged in the IT provider's tickets.
164.310(d)(2)(iii)	Accountability	Partly	Implemented	An asset list kept by the IT provider is reasonable and appropriate.
164.310(d)(2)(iv)	Data Backup and Storage	In place	Implemented	The imaging server was backed up before its move in 2026.
164.312(a)(2)(iii)	Automatic Logoff	In place	Implemented	Screens lock after 15 minutes, 5 at the front desk.
164.312(a)(2)(iv)	Encryption and Decryption	In place	Implemented	BitLocker on 6 of 6 laptops and on the imaging server; the charting vendor encrypts at rest under its business associate agreement.
164.312(c)(2)	Mechanism to Authenticate ePHI	In place	Alternative measure	The charting system's record versioning and audit trail show every change to a record and who made it. Separate checksums are not reasonable for a practice this size.
164.312(e)(2)(i)	Integrity Controls	In place	Implemented	TLS protects data in transit to the charting vendor and the imaging vendor.
164.312(e)(2)(ii)	Encryption	Partly	Implemented	Patients and labs receive patient information by email, so encryption is reasonable and appropriate.

REMEDIATION PLAN (POA&M)

Highest risk first. Risk is likelihood x impact on a five-level scale, rated with the client.

Risk	Ref	Weakness	Planned action	Owner	Due
Very high	164.312(d)	Person or Entity Authentication: MFA on every mailbox and the VPN since Oct 14, 2026. The IT provider's remote-support tool has no MFA.	Turn on MFA in the remote-support tool, or replace the tool	Example Managed IT (made up)	Nov 6, 2026
High	164.308(a)(1)(ii)(D)	Information System Activity Review: Nobody reviews the charting system's access report or Microsoft 365 sign-in activity.	Monthly review of the charting access report and Microsoft 365 sign-in alerts, signed off by the practice administrator	Practice administrator	Jan 29, 2027
High	164.312(b)	Audit Controls: The charting system keeps audit logs, but Microsoft 365 audit logs stay only 90 days and no logs are collected or monitored.	Send Microsoft 365 and firewall logs to the IT provider's monitoring service and keep them at least a year	Example Managed IT (made up)	Feb 26, 2027
High	164.308(a)(1)(ii)(A)	Risk Analysis: The last risk analysis is from 2023, by the previous IT provider. It does not cover the cloud charting system adopted in 2025, the replacement imaging server or Microsoft 365. This assessment is the update.	Finish the updated risk analysis from this assessment and have the managing dentist approve it	Practice administrator	Nov 30, 2026
Moderate	164.308(a)(7)(ii)(C)	Emergency Mode Operation Plan: No procedure for seeing patients while the charting system is down.	Paper downtime procedure with a printed next-day schedule and contacts; test it once	Office manager	Jan 15, 2027
Moderate	164.308(b)(3)	Written Contract or Other Arrangement: No business associate agreement for the online appointment-reminder service, which receives patient names and phone numbers.	Sign a business associate agreement with the reminder service, or stop sending it patient information	Practice administrator	Nov 6, 2026
Moderate	164.308(a)(4)(ii)(B)	Access Authorization: The front-desk role can read clinical notes, which it does not need.	Remove clinical-note access from the front-desk role	Practice administrator	Nov 13, 2026
Moderate	164.308(a)(6)(ii)	Response and Reporting: The Oct 13, 2026 email fraud was handled and documented, but the incident response plan is a September draft, not approved, and has never been exercised.	Approve the incident response plan and run a tabletop exercise	Managing dentist	Nov 20, 2026
Moderate	164.312(e)(2)(ii)	Encryption: Email to patients and labs is encrypted only when staff add the [secure] tag. DMARC is set to p=none.	Turn on automatic encryption for messages with patient information, and move DMARC to quarantine	Example Managed IT (made up)	Nov 30, 2026
Moderate	164.308(a)(1)(ii)(B)	Risk Management: No risk register. Fixes are tracked only as tickets with the IT provider.	Start a risk register from this assessment's gaps and review it every quarter	Practice administrator	Dec 15, 2026

Risk	Ref	Weakness	Planned action	Owner	Due
Moderate	164.312(a)(2)(i)	Unique User Identification: Two shared logins, on the sterilization-room and X-ray workstations.	Replace the shared logins with individual accounts and fast user switching	Example Managed IT (made up)	Dec 15, 2026
Moderate	164.308(a)(4)(ii)(C)	Access Establishment and Modification: Access changes are made on request, but nobody reviews who has access.	Quarterly access review of charting and Microsoft 365 accounts, signed by the managing dentist	Practice administrator	Dec 31, 2026
Moderate	164.308(a)(7)(ii)(B)	Disaster Recovery Plan: The imaging server was restored in a test on Oct 7 (2 hours 40 minutes). Nothing is written for an outage at the charting vendor or the loss of the office network.	Write the disaster recovery steps for a charting vendor outage and for losing the office	Example Managed IT (made up)	Jan 15, 2027
Moderate	164.308(a)(7)	Contingency Plan: Backups and a restore test exist, but there is no single contingency plan.	Pull the backup, disaster recovery and downtime procedures into one contingency plan approved by the managing dentist	Practice administrator	Jan 29, 2027
Moderate	164.308(a)(8)	Evaluation: No evaluation between 2023 and this assessment.	Repeat this assessment every year and after major changes	Practice administrator	Oct 15, 2027
Low	164.310(a)(2)(iii)	Access Control and Validation Procedures: IT provider technicians and the imaging vendor's engineer are not signed in.	Sign in every vendor at the front desk	Office manager	Nov 6, 2026
Low	164.310(d)(2)(iii)	Accountability: The asset list was last updated in November 2025; two replaced workstations are missing from it.	Update the asset inventory and keep it current with each change	Example Managed IT (made up)	Nov 6, 2026
Low	164.310(c)	Workstation Security: The two front-desk screens face the waiting room and have no privacy filters.	Privacy filters on the front-desk screens, and turn them away from the waiting room	Office manager	Nov 13, 2026
Low	164.316(b)(2)(i)	Time Limit: Older policies were thrown away when the 2026 set was approved.	Keep retired versions for six years in the compliance folder	Practice administrator	Nov 30, 2026
Low	164.308(a)(3)(ii)(B)	Workforce Clearance Procedure: Front-desk temps from the staffing agency start before their access is reviewed, and the agency's checks are not confirmed.	Ask the agency to confirm its checks, and review each temp's access before the first shift	Office manager	Dec 15, 2026
Low	164.314(a)(2)(i)(A)	Business Associate Contracts: Comply with the Security Rule: The imaging vendor's 2012 agreement does not require it to comply with the Security Rule.	Replace the imaging vendor's agreement with the current template	Practice administrator	Dec 15, 2026
Low	164.308(a)(7)(ii)(D)	Testing and Revision Procedures: Restore tested Oct 7; the plan itself has not been tested.	Yearly tabletop of the contingency plan	Managing dentist	Mar 31, 2027

RESULTS BY STANDARD

Administrative Safeguards (164.308)

Ref	Item	Status	Finding and evidence
164.308(a)(1)	Standard: Security Management Process	In place	Security policies approved Sep 24, 2026. The gaps are in the specifications below. Evidence: Information security policy v1.0, approved Sep 24, 2026 (compliance folder)
164.308(a)(1)(ii)(A)	Risk Analysis (R)	Partly	The last risk analysis is from 2023, by the previous IT provider. It does not cover the cloud charting system adopted in 2025, the replacement imaging server or Microsoft 365. This assessment is the update. Evidence: Risk analysis 2023 (compliance folder)
164.308(a)(1)(ii)(B)	Risk Management (R)	Partly	No risk register. Fixes are tracked only as tickets with the IT provider.
164.308(a)(1)(ii)(C)	Sanction Policy (R)	In place	Evidence: Employee handbook 2026, section 7.4 (sanctions)
164.308(a)(1)(ii)(D)	Information System Activity Review (R)	Not in place	Nobody reviews the charting system's access report or Microsoft 365 sign-in activity.
164.308(a)(2)	Standard: Assigned Security Responsibility	In place	The practice administrator is the security official, designated in writing. Evidence: Security official designation, signed Sep 24, 2026
164.308(a)(3)	Standard: Workforce Security	In place	Access is requested by the office manager and set up by the IT provider.
164.308(a)(3)(ii)(A)	Authorization and/or Supervision (A)	In place	
164.308(a)(3)(ii)(B)	Workforce Clearance Procedure (A)	Partly	Front-desk temps from the staffing agency start before their access is reviewed, and the agency's checks are not confirmed.
164.308(a)(3)(ii)(C)	Termination Procedures (A)	In place	Evidence: Leaver checklist, last used Sep 15, 2026
164.308(a)(4)	Standard: Information Access Management	In place	Access is granted by role in the charting system.
164.308(a)(4)(ii)(A)	Isolating Health Care Clearinghouse Functions (R)	Not applicable	The practice is not a health care clearinghouse and does not include one.
164.308(a)(4)(ii)(B)	Access Authorization (A)	Partly	The front-desk role can read clinical notes, which it does not need.
164.308(a)(4)(ii)(C)	Access Establishment and Modification (A)	Partly	Access changes are made on request, but nobody reviews who has access.
164.308(a)(5)	Standard: Security Awareness and Training	In place	Evidence: Training completion report, Sep 10, 2026 (14 of 14); phishing test Sep 18, 2026
164.308(a)(5)(ii)(A)	Security Reminders (A)	In place	
164.308(a)(5)(ii)(B)	Protection from Malicious Software (A)	In place	
164.308(a)(5)(ii)(C)	Log-in Monitoring (A)	In place	
164.308(a)(5)(ii)(D)	Password Management (A)	In place	
164.308(a)(6)	Standard: Security Incident Procedures	In place	Staff know to report to the practice administrator; the Oct 13 email fraud was reported within the hour.
164.308(a)(6)(ii)	Response and Reporting (R)	Partly	The Oct 13, 2026 email fraud was handled and documented, but the incident response plan is a September draft, not approved, and has never been exercised. Evidence: Incident record, Oct 13, 2026 (Incident Log file)

Ref	Item	Status	Finding and evidence
164.308(a)(7)	Standard: Contingency Plan	Partly	Backups and a restore test exist, but there is no single contingency plan.
164.308(a)(7)(ii)(A)	Data Backup Plan (R)	In place	Evidence: Backup job report, Sep 30, 2026; immutable copy settings
164.308(a)(7)(ii)(B)	Disaster Recovery Plan (R)	Partly	The imaging server was restored in a test on Oct 7 (2 hours 40 minutes). Nothing is written for an outage at the charting vendor or the loss of the office network.
164.308(a)(7)(ii)(C)	Emergency Mode Operation Plan (R)	Not in place	No procedure for seeing patients while the charting system is down.
164.308(a)(7)(ii)(D)	Testing and Revision Procedures (A)	Partly	Restore tested Oct 7; the plan itself has not been tested.
164.308(a)(7)(ii)(E)	Applications and Data Criticality Analysis (A)	In place	
164.308(a)(8)	Standard: Evaluation	Partly	No evaluation between 2023 and this assessment.
164.308(b)(1)	Standard: Business Associate Contracts and Other Arrangements	In place	Business associate agreements on file for the charting vendor, the IT provider, the imaging vendor, the billing service and the shredding company.
164.308(b)(3)	Written Contract or Other Arrangement (R)	Partly	No business associate agreement for the online appointment-reminder service, which receives patient names and phone numbers. Evidence: Business associate agreements folder (5 of 6 vendors)

Physical Safeguards (164.310)

Ref	Item	Status	Finding and evidence
164.310(a)	Standard: Facility Access Controls	In place	Alarmed suite; the server closet is locked.
164.310(a)(2)(i)	Contingency Operations (A)	In place	
164.310(a)(2)(ii)	Facility Security Plan (A)	In place	Evidence: Facility security plan, Sep 2026
164.310(a)(2)(iii)	Access Control and Validation Procedures (A)	Partly	IT provider technicians and the imaging vendor's engineer are not signed in.
164.310(a)(2)(iv)	Maintenance Records (A)	Not in place	
164.310(b)	Standard: Workstation Use	In place	Evidence: Workstation use policy, approved Sep 24, 2026
164.310(c)	Standard: Workstation Security	Partly	The two front-desk screens face the waiting room and have no privacy filters.
164.310(d)	Standard: Device and Media Controls	In place	
164.310(d)(2)(i)	Disposal (R)	In place	Evidence: Shredding company certificates of destruction, 2026
164.310(d)(2)(ii)	Media Re-use (R)	In place	The IT provider wipes drives before reuse.
164.310(d)(2)(iii)	Accountability (A)	Partly	The asset list was last updated in November 2025; two replaced workstations are missing from it.
164.310(d)(2)(iv)	Data Backup and Storage (A)	In place	

Technical Safeguards (164.312)

Ref	Item	Status	Finding and evidence
164.312(a)	Standard: Access Control	In place	Role-based access in the charting system; the gaps are in the specifications below.
164.312(a)(2)(i)	Unique User Identification (R)	Partly	Two shared logins, on the sterilization-room and X-ray workstations.
164.312(a)(2)(ii)	Emergency Access Procedure (R)	In place	A break-glass administrator account for the charting system, sealed in the safe.
164.312(a)(2)(iii)	Automatic Logoff (A)	In place	
164.312(a)(2)(iv)	Encryption and Decryption (A)	In place	Evidence: Device encryption report, Oct 1, 2026
164.312(b)	Standard: Audit Controls	Not in place	The charting system keeps audit logs, but Microsoft 365 audit logs stay only 90 days and no logs are collected or monitored.
164.312(c)	Standard: Integrity	In place	
164.312(c)(2)	Mechanism to Authenticate ePHI (A)	In place	
164.312(d)	Standard: Person or Entity Authentication	Partly	MFA on every mailbox and the VPN since Oct 14, 2026. The IT provider's remote-support tool has no MFA.
164.312(e)(1)	Standard: Transmission Security	In place	TLS for the charting system and email.
164.312(e)(2)(i)	Integrity Controls (A)	In place	
164.312(e)(2)(ii)	Encryption (A)	Partly	Email to patients and labs is encrypted only when staff add the [secure] tag. DMARC is set to p=none.

Organizational Requirements (164.314)

Ref	Item	Status	Finding and evidence
164.314(a)	Standard: Business Associate Contracts or Other Arrangements	In place	Agreements checked against 164.314(a)(2) on Oct 9.
164.314(a)(2)(i)(A)	Business Associate Contracts: Comply with the Security Rule (R)	Partly	The imaging vendor's 2012 agreement does not require it to comply with the Security Rule.
164.314(a)(2)(i)(B)	Business Associate Contracts: Subcontractors (R)	In place	
164.314(a)(2)(i)(C)	Business Associate Contracts: Report Security Incidents (R)	In place	
164.314(a)(2)(ii)	Other Arrangements (R)	Not applicable	The practice is not a government entity.
164.314(a)(2)(iii)	Business Associate Contracts with Subcontractors (R)	Not applicable	Applies to business associates and their subcontractors; the practice is a covered entity.
164.314(b)	Standard: Requirements for Group Health Plans	Not applicable	The practice is not a group health plan.
164.314(b)(2)(i)	Plan Sponsor Safeguards (R)	Not applicable	Not a group health plan.
164.314(b)(2)(ii)	Adequate Separation (R)	Not applicable	Not a group health plan.
164.314(b)(2)(iii)	Plan Sponsor Agents (R)	Not applicable	Not a group health plan.
164.314(b)(2)(iv)	Plan Sponsor Security Incident Reporting (R)	Not applicable	Not a group health plan.

Policies and Procedures and Documentation Requirements (164.316)

Ref	Item	Status	Finding and evidence
164.316(a)	Standard: Policies and Procedures	In place	Evidence: Policy set v1.0, approved Sep 24, 2026 (Document Register)
164.316(b)	Standard: Documentation	In place	Policies, the security official designation and incident records are kept in the compliance folder. Addressable decisions are recorded for the first time in this assessment.
164.316(b)(2)(i)	Time Limit (R)	Partly	Older policies were thrown away when the 2026 set was approved.
164.316(b)(2)(ii)	Availability (R)	In place	On the shared drive and in the staff handbook.
164.316(b)(2)(iii)	Updates (R)	In place	A yearly review date is set for each document in the Document Register.

SOURCES AND LIMITATIONS

Source: NIST SP 800-66 Rev. 2, Implementing the HIPAA Security Rule (NIST CPRT). Safeguards, standards, key activities and sample questions are NIST's wording from NIST SP 800-66 Rev. 2, Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide (<https://csrc.nist.gov/pubs/sp/800/66/r2/final>), exported from the NIST CPRT on Oct 19, 2026. Implementation specification names, citations and Required/Addressable status are from the HIPAA Security Rule, 45 CFR Part 164, Subpart C. NIST does not endorse MansioSec. NIST CSF 2.0 links: Source: HHS Office for Civil Rights, HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework (February 2016), converted to CSF 2.0 with NIST's references. Neither HHS nor NIST endorses MansioSec.

Evidence is listed by name or location; the documents stay with the client. The findings describe systems and processes, and no protected health information belongs in this report.