

SAMPLE DELIVERABLE

Compliance Readiness: HIPAA Gap Report

Control-by-control readiness for a HIPAA Security Rule audit, with a prioritized action plan.

SAMPLE Fictional demonstration data · Prepared by Arcline

PREPARED FOR

Brightwell Dental Group

Dental / healthcare (HIPAA-covered entity) · 3 locations · 38 staff · 5 servers

Network, endpoints, access controls, backups, email security, and remote access, assessed across all three locations.

01 Readiness summary

62%

PARTIAL READINESS

7

READY

7

PARTIAL

2

GAPS

This report measures how ready Brightwell Dental Group is for a HIPAA Security Rule audit, control by control, based on the technical review completed in July 2026. It does not certify anything; the goal is to show exactly where the gaps are so the practice can close them before an auditor, insurer, or client asks. Of the sixteen controls reviewed, most are in place or close to it. The two real gaps (no multi-factor authentication and no audit logging) match the two highest-priority findings in the Security Risk Assessment, and closing those findings closes most of the compliance gap at the same time.

02 Control status

Readiness for the HIPAA Security Rule, control by control. Status reflects the technical review, not a formal audit.

CONTROL DOMAIN	STANDARD	STATUS	NOTES
Risk Management	164.308(a)(1)(ii)	PARTIAL	A formal security risk analysis was completed recently, but findings are not yet tracked through to closure.
Information Access Management	164.308(a)(4)(i)	READY	Access to patient records is limited to staff with a legitimate need, by role.
Workforce Security	164.308(a)(3)(i)	PARTIAL	Access levels are assigned by role, but there is no formal offboarding checklist that revokes access on the day someone leaves.
Contingency Plan: Backup	164.308(a)(7)(ii)	PARTIAL	Backups run nightly, but restores are not tested (see finding F-04).
Evaluation	164.308(a)(8)	READY	The practice reviews its security program annually with its managed IT provider.
Facility Access Controls	164.310(a)(1)	PARTIAL	Server rooms are locked, but visitor sign-in is inconsistent across the three locations.
Workstation Use & Security	164.310(b), (c)	READY	Workstations lock automatically after 5 minutes; screens are not visible from waiting areas.
Access Control: Unique User IDs	164.312(a)(2)(i)	PARTIAL	Most staff have unique logins, but several administrator accounts are shared (see finding F-02).
Access Control: Emergency Access	164.312(a)(2)(ii)	READY	A documented emergency-access procedure is in place for the practice management system.

CONTROL DOMAIN	STANDARD	STATUS	NOTES
Access Control: Automatic Logoff	164.312(a)(2)(iii)	READY	Automatic logoff applies after 10 minutes of inactivity on practice systems.
Audit Controls	164.312(b)	GAP	No centralized logging or audit trail of who accessed what, and when (see finding F-07).
Integrity	164.312(c)(1)	PARTIAL	Electronic protected health information is not protected end-to-end against unauthorized alteration.
Person or Entity Authentication	164.312(d)	GAP	No multi-factor authentication on remote access or administrator accounts (see finding F-02).
Transmission Security: Encryption	164.312(e)(1)(ii)	READY	All data in transit to and from the practice is encrypted (TLS).
Business Associate Agreements	164.314(a)(1)(i)	READY	BAAs are in place with the email provider, EHR vendor, and IT provider.
Policies & Documentation Retention	164.316(b)(1)	PARTIAL	Security policies exist, but a few are outdated and not all are retained for the required 6 years.

03 Action plan

The gaps and partial controls, in the order they should be closed. Most overlap directly with the Security Risk Assessment findings.

PRIORITY	CONTROL	ACTION	RELATED
P1	Person or Entity Authentication (164.312(d))	Enable multi-factor authentication on all remote access and administrator accounts; replace shared admin logins with unique accounts.	See finding F-02
P1	Audit Controls (164.312(b))	Stand up centralized logging with a 12-month retention policy covering servers, workstations, and the VPN.	See finding F-07
P2	Contingency Plan: Backup (164.308(a)(7)(ii))	Run and document a quarterly backup restore drill.	See finding F-04
P2	Workforce Security (164.308(a)(3)(i))	Add an offboarding checklist that revokes access and collects keys/devices on the last day of employment.	None
P3	Facility Access Controls (164.310(a)(1))	Standardize visitor sign-in and escorting across all three locations.	None
P3	Policies & Documentation (164.316(b)(1))	Refresh outdated policies and set up a 6-year retention folder for security documentation.	None

HOW TO READ THIS

Arcline does not certify compliance: the goal of this report is to get the practice ready so a real audit isn't a scramble. Close the P1 items first: they are the same fixes as the top findings in the risk assessment, and they move most of the readiness score on their own.