



Dental HIPAA Security Risk Analysis & Policy Kit

Security risk analysis workbook, asset inventory, risk register and written security policies for dental practices and labs.

What's inside

File	What it is / how to use it
01_Dental_HIPAA_Security_Workbook.xlsx	Asset inventory, risk analysis with likelihood x impact scoring, safeguard checklist by section, BAA tracker, training log, access review and incident log.
02_Security_Policies.docx	Written policies to adapt.
03_Risk_Analysis_Report.docx	Summary report for your file.
04_Incident_Response_Checklist.docx	Step-by-step checklist.

Templates, not legal advice and not regulatory advice. Public regulation text (45 CFR Parts 160 and 164, HHS OCR guidance) is summarized with sources named. The HIPAA Security Rule changes proposed in January 2025 were not final when this kit was written (Oct 2026); the kit follows the rule currently in effect. Use qualified legal and IT support for breach decisions and compliance.

About the author

Built by Matt Norman, US Navy veteran and former SpaceX Falcon 9 quality inspector and QA supervisor. (Not affiliated with or endorsed by SpaceX.) Norman Quality Tools is Veteran-Owned & Operated. Contains no SpaceX, government, or customer proprietary information; all example data is made up.

License

One company license: use and edit at all sites of the purchasing company. Do not resell or redistribute. Works with Word/Excel 2016+, Microsoft 365, LibreOffice; no macros. Norman Quality Tools (Veteran-Owned & Operated), 600 W Santa Ana Blvd, Ste 114-A3064, Santa Ana, CA 92701. Support: normanqualitytools.com/support.html

Dental HIPAA Security Risk Analysis & Policy Kit v1, Rev A (2026-10). Independent guidance. Not affiliated with or endorsed by the U.S. HHS, OCR, the ADA, SAE International, IAQG, ISO, or any current or former employer of the author. Standard clause numbers are for navigation only; buy standards from their publishers. Not legal advice; does not guarantee certification or approval. Templates, not legal advice and not regulatory advice. © 2026 Norman Quality Tools. All rights reserved. Licensed for use within the purchasing company; do not resell or redistribute.

HIPAA Security Policy Set (dental)

Dental HIPAA Security Risk Analysis & Policy Kit - Document 02 - Rev A (2026-10)

Practice		Security official	
Effective date			

Edit each policy to match how your office actually works. Keep policies and changes for 6 years (45 CFR 164.316).

1. Security management

[Practice] performs a security risk analysis at least annually and after major changes (new software, move, breach), and tracks actions in the Risk Analysis sheet.

2. Workforce access

Each person gets a unique login with only the access their job needs. Access is removed on the last day of work. The security official reviews access each quarter.

3. Passwords and MFA

[Set your rules: length, MFA for email, remote access and cloud systems.]

4. Workstations and devices

Screens lock after [X] minutes. Laptops and phones that hold ePHI are encrypted. Lost devices are reported the same day.

5. Backup and contingency

[Backup schedule, offline/immutable copy, restore test frequency, who to call.]

6. Email and texting

[When encryption is used; patient-requested unencrypted communication and how it is documented.]

7. Vendors

No vendor gets ePHI without a signed business associate agreement on the BAA Tracker.

8. Incidents

Report suspected incidents to the security official at once. The security official logs it and decides if it is a breach using the Incident Log.

9. Media disposal

Drives, sensors and paper with ePHI are wiped or destroyed and logged before disposal or re-use.

Role	Name	Signature	Date
Security official			
Owner / dentist			