

SAMPLE DELIVERABLE

Remediation Recommendations

Each finding mapped to a concrete fix, owner, and order of work, in plain English.

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.

This plan takes the findings from the Security Risk Assessment and turns each one into a concrete action: who does it, how much effort it is, and by when. Work through the priorities in order; each group builds on the one before it. Most of this is routine IT hygiene that can be completed in the first month.

01 Priorities at a glance

PRIORITY	FINDING	OWNER	TIMELINE	EFFORT
P1	F-01: Patch the VPN appliance and enable automatic updates	IT	7 days	Low
P1	F-02: Turn on multi-factor authentication	IT	14 days	Low-Medium
P2	F-03: Publish SPF, enable DKIM, and add DMARC	IT	14 days	Low
P3	F-04: Test backup restores quarterly	IT	30 days	Medium
P3	F-05: Bring workstations up to date	IT	30 days	Low-Medium
P4	F-06: Separate guest Wi-Fi	IT	90 days	Low
P4	F-07: Centralize and retain logs	IT	90 days	Medium

02 The plan, priority by priority

Close the two doors an attacker would walk through first

PRIORITY 1

Within 7 days · These are the findings most likely to turn into a real incident. Both are quick to fix, and both remove the most common paths ransomware uses to get in.

F-01: Patch the VPN appliance and enable automatic updates

Install the latest firmware on the edge VPN appliance, enable automatic security updates, and add it to the monthly patch review.

Owner: IT · Timeline: 7 days · Effort: Low

F-02: Turn on multi-factor authentication

Require MFA for all remote access and all administrator accounts; issue each person a unique admin account. Allow a two-week enrollment window for staff phones.

Owner: IT · Timeline: 14 days · Effort: Low-Medium

Stop email impersonation of the practice

PRIORITY 2

Within 14 days · Spoofed emails are how most phishing and ransomware reaches staff. Publishing three DNS records closes the door on mail that looks like it comes from you.

F-03: Publish SPF, enable DKIM, and add DMARC

Publish a strict SPF record, enable DKIM signing on the mail provider, and publish a DMARC record starting at p=none, tightened to quarantine over a few weeks.

Owner: IT · Timeline: 14 days · Effort: Low

Make sure recovery actually works

PRIORITY 3

Within 30 days · A backup that has never been restored is a hope, not a plan. Outdated workstations are the most common way ransomware enters a small business. Both are fixed with routine, low-cost habits.

F-04: Test backup restores quarterly

Run a quarterly restore drill: restore a sample of patient records, one full mailbox, and one whole server, and document the result.

Owner: IT · Timeline: 30 days · Effort: Medium

F-05: Bring workstations up to date

Enable automatic updates on all workstations, upgrade or replace the four machines past end-of-support, and add a monthly 15-minute patch review.

Owner: IT · Timeline: 30 days · Effort: Low-Medium

Hygiene that compounds over time

PRIORITY 4

Within 90 days · recurring · None of these are urgent on their own, but each is cheap and reduces risk a little more, and together they make the practice an easier story to tell to insurers and auditors.

F-06: Separate guest Wi-Fi

Add an isolated guest Wi-Fi network with its own password at all three locations, kept away from internal systems and patient records.

Owner: IT · Timeline: 90 days · Effort: Low

F-07: Centralize and retain logs

Collect logs centrally from servers, workstations, and network equipment, and retain them for at least 12 months.

Owner: IT · Timeline: 90 days · Effort: Medium

03 Ongoing hygiene

The practices below keep the fixes in this plan from quietly unravelling.

- **Monthly:** 15-minute patch review across servers, workstations, and the VPN appliance.
- **Quarterly:** backup restore drill, with the result documented and kept on file.
- **Annually:** re-run the security risk assessment to confirm the posture has improved and catch anything new.

04 What can wait

LOWER-PRIORITY ITEMS

Nothing in Priority 4 is urgent on its own. If you only act on Priorities 1–3 this quarter, you will have closed the doors that matter most. The Priority 4 items are cheap and worth doing before your next insurance or compliance review, not because anything is broken, but because they make the practice visibly easier to defend.