

SAMPLE DELIVERABLE

Security Risk Assessment: Findings Report

A written, prioritized summary of what we found and what to fix first.

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 Executive summary

Moderate

OVERALL POSTURE

2

HIGH FINDINGS

3

MEDIUM FINDINGS

2

LOW FINDINGS

This report summarizes a security risk assessment of Brightwell Dental Group, completed in July 2026. We reviewed the network and firewall, staff workstations and servers, how people sign in to systems, the backup setup, and how email is protected. The goal was to find the weak spots an attacker or a ransomware incident would hit first, not to grade your team.

Overall, your environment is in reasonable shape: your firewall rules are sensible, every workstation has endpoint protection, and email is filtered. Nothing we found suggests an active breach. But a handful of issues deserve attention, and two of them (an unpatched VPN appliance and missing multi-factor authentication) are the kind of thing that leads directly to a ransomware incident. We rate your overall posture as **Moderate**: acceptable for day-to-day operations, with a few gaps worth closing before you are targeted.

WHAT'S GOING WELL

- Firewall rules are reviewed, and only the ports that need to be exposed are exposed
- Endpoint protection is installed and updating on every workstation
- Email is filtered for spam and known phishing before it reaches staff
- Backups run automatically every night
- No evidence of an active breach or compromise was found

TOP PRIORITIES

1. Patch the VPN appliance and turn on automatic updates
2. Turn on multi-factor authentication for remote access and admin accounts
3. Publish the email authentication records (SPF / DKIM / DMARC)

02 Prioritized findings

Every finding, ranked by how urgently it should be addressed. Details follow in the next section.

ID	FINDING	SEVERITY	OWNER	TIMELINE
F-01	Unpatched VPN appliance on the network edge	HIGH	IT	within 7 days
F-02	No multi-factor authentication on remote access or admin accounts	HIGH	IT	within 14 days
F-03	Email authentication records incomplete (SPF / DMARC)	MEDIUM	IT	within 30 days
F-04	Backup restores have not been tested	MEDIUM	IT	within 30 days

ID	FINDING	SEVERITY	OWNER	TIMELINE
F-05	Workstations running outdated software	MEDIUM	IT	within 30 days
F-06	Office Wi-Fi has no guest network	LOW	IT	within 90 days
F-07	No centralized logging or log retention	LOW	IT	within 90 days

03 Detailed findings

F-01 · Unpatched VPN appliance on the network edge

HIGH

Affected: Edge VPN appliance (brightwell-vpn, 10.0.10.1) · Owner: IT · within 7 days

- WHY IT MATTERS** If an attacker exploits a known vulnerability in this appliance, they could get inside your network and start moving toward patient records and business systems. VPN appliances are one of the most common entry points for ransomware.
- WHAT WE FOUND** The VPN appliance that lets staff connect remotely is running an older firmware release with known security issues. It is not set to install security updates automatically, and the last update was applied several months ago. This is a classic “patch it now” situation: the fix is straightforward, but the window matters.
- EVIDENCE** Firmware version 9.6.2 detected on the edge appliance (brightwell-vpn). Vendor advisories for this release are outstanding; automatic updates are disabled.
- RECOMMENDATION** Patch the appliance to the latest firmware and enable automatic security updates. Add it to a monthly patch-review cycle.

F-02 · No multi-factor authentication on remote access or admin accounts

HIGH

Affected: Remote-access VPN and all administrator accounts · Owner: IT · within 14 days

- WHY IT MATTERS** A password is currently the only thing standing between an attacker and full administrator access. If one is stolen, guessed, or reused from a breach elsewhere, nothing stops them from signing in as an administrator.
- WHAT WE FOUND** Remote access to the network requires only a username and password. Administrator accounts on servers and workstations also rely on passwords alone, and a few staff share a common admin login. Multi-factor authentication (a code from a phone app or a security key) is the single most effective control you can add.
- EVIDENCE** Password-only authentication observed on the VPN portal and on domain administrator accounts. No MFA policy documented.
- RECOMMENDATION** Enable MFA on all remote access and all administrator accounts, and issue a unique admin account to each person who needs one. Give staff a two-week grace period to enroll their phones.

F-03 · Email authentication records incomplete (SPF / DMARC)**MEDIUM**

Affected: brightwelldental.com email domain · Owner: IT · within 30 days

- WHY IT MATTERS** Attackers can send emails that look like they come from your practice. This is how most phishing and ransomware starts: a convincing email “from the front desk” that isn’t from you at all.
- WHAT WE FOUND** The practice’s email domain doesn’t publish the records that let receiving mail servers verify whether an email really came from you. There is no DMARC record at all, and the SPF record is too permissive to be meaningful. The fix is three short DNS records.
- EVIDENCE** No DMARC record found for brightwelldental.com. SPF record present but permissive (all).
- RECOMMENDATION** Publish a strict SPF record, enable DKIM signing on your mail provider, and add a DMARC record starting at p=none, then tighten it to quarantine over a few weeks once you confirm legitimate mail is unaffected.

F-04 · Backup restores have not been tested**MEDIUM**

Affected: All systems (patient records, practice-management software, file server) · Owner: IT · within 30 days

- WHY IT MATTERS** If ransomware hit, you would be relying on backups that nobody has proved actually restore. Restore failures almost always surface at the worst possible moment.
- WHAT WE FOUND** Nightly backups are running and the job logs look healthy, but nobody has actually restored from them in over a year. A backup that has never been tested is a hope, not a plan. A single quarterly restore drill changes that.
- EVIDENCE** Backup job logs show successful nightly backups. No restore drill documented in the past 12 months.
- RECOMMENDATION** Schedule a quarterly restore drill: restore a sample of patient records, a full mailbox, and one whole server from backup, and document the result.

F-05 · Workstations running outdated software**MEDIUM**

Affected: 24 of 38 staff workstations; 4 past end-of-support · Owner: IT · within 30 days

- WHY IT MATTERS** Outdated operating systems and applications are the most common way ransomware gets into a small business. A single unpatched machine can be enough.
- WHAT WE FOUND** A scan found 24 workstations missing recent security updates, and four are running an operating system the vendor no longer supports, so they will never receive updates again. Most of this is simple to resolve with automatic updates.
- EVIDENCE** Patch scan: 24/38 workstations missing updates; 4 running an OS past end-of-support.
- RECOMMENDATION** Turn on automatic updates everywhere, upgrade or replace the four unsupported machines, and add a monthly 15-minute patch review to your routine.

F-06 · Office Wi-Fi has no guest network

LOW

Affected: All 3 office locations · Owner: IT · within 90 days

WHY IT MATTERS Every visitor's phone and laptop joins the same Wi-Fi your practice computers use. One infected visitor device can reach systems holding patient records.

WHAT WE FOUND At all three locations, the only Wi-Fi network is shared between staff and guests. Separating visitors onto their own network is cheap, quick, and keeps their devices away from your internal systems.

EVIDENCE Single shared SSID observed at all three offices.

RECOMMENDATION Add a separate guest Wi-Fi network (its own password, isolated from internal systems) at each location.

F-07 · No centralized logging or log retention

LOW

Affected: Servers, workstations, network equipment · Owner: IT · within 90 days

WHY IT MATTERS If something does go wrong, there is no reliable record of what happened, which makes it much harder to find and fix the cause.

WHAT WE FOUND Logs are stored on each device individually and aren't collected in one place or kept for any defined period. Centralized logging is also something most cyber-insurance and compliance reviewers expect to see.

EVIDENCE No central log collection or retention policy found.

RECOMMENDATION Set up central log collection and retain logs for at least 12 months. If you subscribe to managed monitoring, this is included.

04 Remediation roadmap

The full, owner-by-owner action plan is in the separate Remediation Recommendations document. The table below shows the order of work.

ID	FINDING	FIX	OWNER	TIMELINE
F-01	Unpatched VPN appliance on the network edge	Patch the appliance to the latest firmware and enable automatic security updates. Add it to a monthly patch-review cycle.	IT	within 7 days
F-02	No multi-factor authentication on remote access or admin accounts	Enable MFA on all remote access and all administrator accounts, and issue a unique admin account to each person who needs one. Give staff a two-week grace period to enroll their phones.	IT	within 14 days
F-03	Email authentication records incomplete (SPF / DMARC)	Publish a strict SPF record, enable DKIM signing on your mail provider, and add a DMARC record starting at p=none, then tighten it to quarantine over a few weeks once you confirm legitimate mail is unaffected.	IT	within 30 days

ID	FINDING	FIX	OWNER	TIMELINE
F-04	Backup restores have not been tested	Schedule a quarterly restore drill: restore a sample of patient records, a full mailbox, and one whole server from backup, and document the result.	IT	within 30 days
F-05	Workstations running outdated software	Turn on automatic updates everywhere, upgrade or replace the four unsupported machines, and add a monthly 15-minute patch review to your routine.	IT	within 30 days
F-06	Office Wi-Fi has no guest network	Add a separate guest Wi-Fi network (its own password, isolated from internal systems) at each location.	IT	within 90 days
F-07	No centralized logging or log retention	Set up central log collection and retain logs for at least 12 months. If you subscribe to managed monitoring, this is included.	IT	within 90 days