

CYBERSECURITY ASSESSMENT REPORT

Business: Chiropractic01
Industry: Healthcare
Employees: 7
Date: {{TODAY}}
Consultant: Timothy Corrado — Cybersecurity Analyst

Executive Summary

This assessment provides a high-level evaluation of **Chiropractic01**'s cybersecurity posture.

The business demonstrates several strong security practices already in place; however, multiple **high-severity risks** were identified that could expose patient data, enable ransomware attacks, or create HIPAA compliance issues if not addressed.

Security Snapshot

Category	Score
Overall Security Score	56 / 100
Network Security	5 / 10
Access Controls	4 / 10
Device Security	6 / 10
Business Processes	9 / 10

Severity Legend

- **High Severity** – Immediate attention required
- **Medium Severity** – Important improvement
- **Unknown** – Status not confirmed; may represent hidden risk
- ✓ **Secure / In Place** – Configured correctly; no action required

Top Risks

- **High Severity** Wi-Fi is not using WPA2 or WPA3 encryption
- **High Severity** Shared user accounts and local admin access in use
- **High Severity** Multi-Factor Authentication not enabled
- **High Severity** No offsite backups available
- **High Severity** Physical access to servers and workstations is unrestricted

Quick Wins (Complete Within 72 Hours)

- Enable **WPA2/WPA3** encryption on all Wi-Fi networks
- Create **unique user accounts** for each employee
- Enable **MFA on email accounts**
- Restrict **server room access**
- Confirm **guest Wi-Fi isolation**

Detailed Findings

Network / Wi-Fi

- Router firmware updated:
✓ **Secure / In Place**
 - Router admin password strong:
✓ **Secure / In Place**
 - WPA2 or WPA3 in use:
● **High Severity**
 - Guest Wi-Fi exists:
✓ **Secure / In Place**
 - Guest Wi-Fi isolated:
○ **Unknown**
 - SSID names recorded:
○ **Unknown**
 - Wi-Fi password complexity strong:
✓ **Secure / In Place**
 - WPS disabled:
○ **Unknown**
 - UPnP disabled:
○ **Unknown**
 - Firewall enabled on router:
✓ **Secure / In Place**
-

Devices / Workstations

- Windows updates current:
✓ **Secure / In Place**
 - Antivirus active:
✓ **Secure / In Place**
 - Local admin disabled:
● **High Severity**
 - BitLocker enabled:
○ **Unknown**
 - Auto-lock screen enabled:
✓ **Secure / In Place**
 - Shared accounts in use:
● **High Severity**
 - RDP enabled anywhere:
○ **Unknown**
 - Unsupported OS present:
✓ **Secure / In Place**
 - USB ports restricted:
✓ **Secure / In Place**
-

Accounts & Access Control

- Unique accounts per employee:
● **High Severity**
- Password complexity enforced:
✓ **Secure / In Place**
- Password expiration policy active:
✓ **Secure / In Place**
- MFA on email:
● **High Severity**
- MFA on critical systems:
● **High Severity**
- Inactive accounts removed:

✓ **Secure / In Place**

- Default accounts disabled:

✓ **Secure / In Place**

Backups & Data Protection

- Backups occur regularly:
 - **Unknown**
 - Backups stored offsite:
 - **High Severity**
 - Backup integrity tested:
 - **Unknown**
 - Shared folders restricted:
 - ✓ **Secure / In Place**
 - Everyone permissions found:
 - ✓ **Secure / In Place**
-

Business Processes & Human Factors

- Incident response plan exists:
 - ✓ **Secure / In Place**
 - Cybersecurity training done:
 - ✓ **Secure / In Place**
 - Onboarding documented:
 - ✓ **Secure / In Place**
 - Offboarding documented:
 - ✓ **Secure / In Place**
-

Physical Security

- Networking equipment secured:
 - ✓ **Secure / In Place**
 - Server room restricted:
 - **High Severity**
 - Workstations not publicly exposed:
 - **High Severity**
-

Unknown Items (Requires Verification)

- Guest Wi-Fi isolation
 - SSID inventory
 - WPS configuration
 - UPnP configuration
 - BitLocker disk encryption
 - RDP exposure
 - Backup frequency
 - Backup integrity testing
-

Short-Term Recommendations (0–30 Days)

- Enable WPA2/WPA3 Wi-Fi encryption
- Enforce unique user accounts
- Enable MFA on all email accounts
- Restrict physical access to servers

- Implement offsite backups
-

Long-Term Improvements (30–180 Days)

- Deploy full-disk encryption (BitLocker)
 - Centralize identity management
 - Implement backup testing schedule
 - Perform annual cybersecurity review
-

Consultant

Timothy Corrado

Cybersecurity Analyst

Email: TimothyCorrado@gmail.com

LinkedIn: <https://linkedin.com/in/timothy-corrado>

END OF REPORT
