

EXAMPLE SECURITY PARTNERS

SECURITY BASELINE ASSESSMENT

CISA Cybersecurity Performance Goals 2.0 (CPG 2.0)

Prepared for

Sample Dental Group (made up)

Assessment period: September 21, 2026 – October 2, 2026

Report date: October 16, 2026

Sector: Healthcare (dental practice)

Prepared by Alex Sample, CISSP

vCISO · Security Consultant · Incident Response Advisor

hello@example.com · example.com

CONFIDENTIAL – CONTAINS SENSITIVE SECURITY INFORMATION ABOUT SAMPLE DENTAL GROUP (MADE UP). DISTRIBUTE ONLY TO AUTHORIZED PERSONNEL.

1. EXECUTIVE SUMMARY

OVERALL POSTURE

Sample Dental Group (made up) has implemented 9 of 34 applicable CISA Cybersecurity Performance Goals (CPG 2.0; 26%). 25 goals are documented as findings in this report.

The basics most often tied to HIPAA are in place: a signed policy, training for every staff member, encrypted devices, separate admin accounts and tested backups. The gaps are the controls that stop an email takeover or ransomware from spreading: MFA is incomplete, the network is flat, logs are not collected, and the incident plan has never been approved or rehearsed.

AT A GLANCE

Applicable goals	Implemented	In progress	Scoped	Not implemented
34	9 (26%)	15 (44%)	2 (6%)	8 (24%)

TOP PRIORITIES

These actions reduce the most risk for the least cost and effort. Each is detailed in Section 4.

#	Action	Goal	Priority	Target
1	Finish and approve the incident response plan, with the insurer's breach line and the HHS notice steps, and run a one-hour ransomware tabletop exercise with the partners, the office manager and the IT provider before the insurance renewal.	1.C Manage Incident Response Plans	High	30 days
2	Give each staff member their own imaging login and retire the shared accounts.	3.C Create Unique Credentials	High	30 days
3	Turn on Microsoft 365 risky sign-in and failed-login alerts and send them to the IT provider and the practice administrator.	3.E Monitor Unsuccessful (Automated) Login Attempts	High	30 days
4	Enforce MFA on every mailbox and on the remote-support tool this month; use number matching or security keys.	3.F Implement Multi-factor Authentication	High	30 days
5	Limit the scanned-forms share to the front desk and office manager, and move forms into the PMS where possible.	3.K Utilize Strong Encryption	High	30 days

RECOMMENDED NEXT STEP

Enforce MFA on every mailbox and on the remote-support tool, and close the firewall admin page to the internet, within 30 days. Both are low-cost changes the IT provider can make this month.

2. SCOPE AND METHODOLOGY

SCOPE

Both offices, 14 staff, 22 endpoints, the imaging server, Microsoft 365, the cloud practice-management system (PMS) and the IT provider's remote access.

Out of scope: The PMS vendor's own systems and personal devices that do not get practice email.

No operational technology (OT) was in scope; OT-specific goals are marked not applicable.

FRAMEWORK

The assessment measured the organization against the Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Performance Goals 2.0 (CPG 2.0), published in December 2025: 34 voluntary, high-impact security practices for information technology (IT) and operational technology (OT), grouped by the six functions of the NIST Cybersecurity Framework 2.0: Govern, Identify, Protect, Detect, Respond and Recover. CISA rates each goal's cost, impact and ease of implementation; these ratings inform the priorities in this report.

Source: CISA, Cybersecurity Performance Goals 2.0. Goal names, outcomes and recommended actions are quoted from CISA.

APPROACH

- Interviews with the managing dentist, the practice administrator, the office manager and the IT provider's account engineer.
- Review of documentation, including the Information Security Policy, training records, backup and restore logs, business associate agreements and the IT provider's patch and endpoint reports.
- Observation: walk-through of both offices, review of Microsoft 365 security settings, an outside check of the practice's internet-facing addresses, and a witnessed restore test.
- Structured scoring of each goal against CISA's stated outcome and recommended action, followed by independent analysis and prioritization by the assessor

STATUS DEFINITIONS

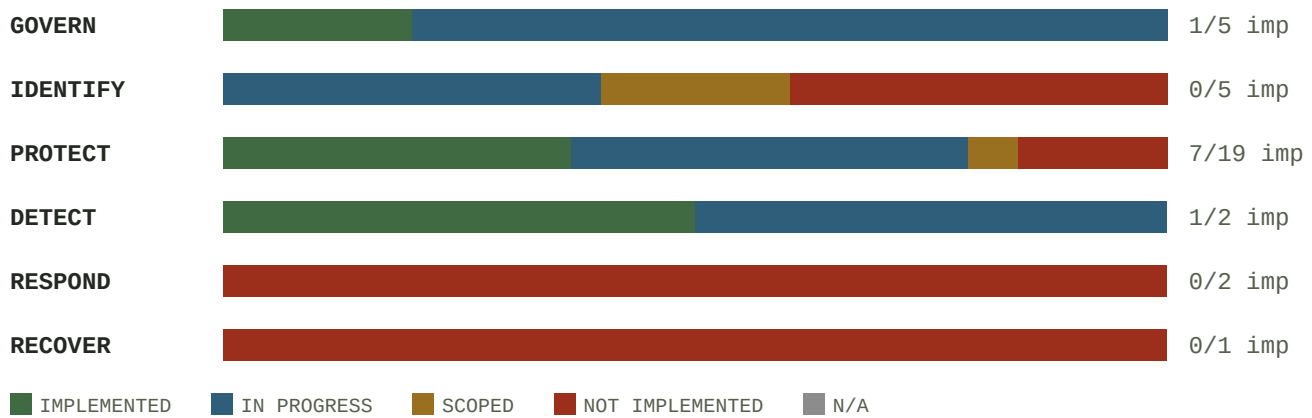
Status	Meaning
Implemented	The practice is in place and operating, with evidence observed or provided.
In progress	Work has started but the practice is not yet fully in place.
Scoped	Planned and resourced, but not yet started.
Not implemented	The practice is not in place.
Not applicable	The practice does not apply to this environment.

LIMITATIONS

This is a point-in-time assessment based on information provided and observed during the assessment period. It is not a penetration test, a technical configuration audit, or a guarantee against compromise. Conditions may change

after the report date.

3. RESULTS BY FUNCTION



Function	Implemented	In progress	Scoped	Not impl.	Applicable
Govern	20%	80%	0%	0%	5
Identify	0%	40%	20%	40%	5
Protect	37%	42%	5%	16%	19
Detect	50%	50%	0%	0%	2
Respond	0%	0%	0%	100%	2
Recover	0%	0%	0%	100%	1
Overall	26%	44%	6%	24%	34

WHAT THIS MEANS

Protect and Detect are the strongest functions, and Identify, Respond and Recover the weakest. Most gaps can be closed by the IT provider within its current agreement; network separation and log collection are the only items that need new spending.

4. FINDINGS

Each finding is a goal assessed as not implemented, in progress, or scoped, ordered by priority. Priority combines CISA's impact and ease-of-implementation ratings with the assessor's judgment of the organization's likely attack paths.

F-01 MANAGE INCIDENT RESPONSE PLANS

CPG goal	1.C Manage Incident Response Plans (CSF 2.0 function: Govern)
Status	In progress
Priority	High
CISA rating	Cost Low · Impact High · Ease Moderate
CISA outcome	Identify improvements by practicing cybersecurity and incident response (IR) plans to maintain and update the organization's cybersecurity program.
Observation	An incident response plan was drafted with the IT provider in September. It is not approved and has never been rehearsed.
Evidence reviewed	DOC-010 Incident Response Plan (draft)
Risk	Without an approved, practised plan, the first hours of an incident are lost to deciding who calls whom, and notice deadlines can be missed.
Recommendation	Finish and approve the incident response plan, with the insurer's breach line and the HHS notice steps, and run a one-hour ransomware tabletop exercise with the partners, the office manager and the IT provider before the insurance renewal.
Owner	Practice administrator
Target	30 days

F-02 CREATE UNIQUE CREDENTIALS

CPG goal	3.C Create Unique Credentials (CSF 2.0 function: Protect)
Status	In progress
Priority	High
CISA rating	Cost Low · Impact High · Ease Simple
CISA outcome	Adversaries are unable to reuse compromised credentials to move laterally across the organization, particularly between IT and OT networks.
Observation	Each person has their own Microsoft 365 and PMS account, but two shared front-desk logins are used on the imaging PCs.

F-02 CREATE UNIQUE CREDENTIALS

Evidence reviewed	None linked
Risk	Shared logins hide who did what and are rarely changed when staff leave.
Recommendation	Give each staff member their own imaging login and retire the shared accounts.
Owner	Office manager
Target	30 days

F-03 MONITOR UNSUCCESSFUL (AUTOMATED) LOGIN ATTEMPTS

CPG goal	3.E Monitor Unsuccessful (Automated) Login Attempts (CSF 2.0 function: Protect)
Status	In progress
Priority	High
CISA rating	Cost Moderate · Impact High · Ease Moderate
CISA outcome	Protect organizations from automated, credential-based attacks.
Observation	Accounts lock after 10 failed attempts, but nobody is alerted to repeated failures or risky sign-ins.
Evidence reviewed	None linked
Risk	Password-guessing and stolen-password sign-ins go unnoticed until money or data is gone.
Recommendation	Turn on Microsoft 365 risky sign-in and failed-login alerts and send them to the IT provider and the practice administrator.
Owner	IT provider
Target	30 days

F-04 IMPLEMENT MULTI-FACTOR AUTHENTICATION

CPG goal	3.F Implement Multi-factor Authentication (CSF 2.0 function: Protect)
Status	In progress
Priority	High
CISA rating	Cost Moderate · Impact High · Ease Moderate
CISA outcome	Add a critical, additional layer of security to protect assets accounts.
Observation	MFA (app approval) is on for 11 of 14 mailboxes. It is off for 3 front-desk mailboxes and on the

F-04 IMPLEMENT MULTI-FACTOR AUTHENTICATION

	IT provider's remote-support tool.
Evidence reviewed	DOC-007 Password and MFA standard (draft)
Risk	Email takeover is the most common cause of payment fraud and patient-data breaches at small practices.
Recommendation	Enforce MFA on every mailbox and on the remote-support tool this month; use number matching or security keys.
Owner	Practice administrator
Target	30 days

F-05 UTILIZE STRONG ENCRYPTION

CPG goal	3.K Utilize Strong Encryption (CSF 2.0 function: Protect)
Status	In progress
Priority	High
CISA rating	Cost Moderate · Impact High · Ease Complex
CISA outcome	Encryption is deployed to maintain confidentiality and integrity of sensitive data across the organization's network to protect from unauthorized access.
Observation	BitLocker is on every device and email and the PMS use TLS. Scanned intake forms sit on a file share every staff account can read.
Evidence reviewed	DOC-004 Device encryption compliance report (IT provider)
Risk	Any compromised account exposes every scanned form, which would be a reportable breach.
Recommendation	Limit the scanned-forms share to the front desk and office manager, and move forms into the PMS where possible.
Owner	IT provider
Target	30 days

F-06 SECURE INTERNET FACING DEVICES

CPG goal	3.S Secure Internet Facing Devices (CSF 2.0 function: Protect)
Status	In progress
Priority	High
CISA rating	Cost Moderate · Impact High · Ease Complex
CISA outcome	Unauthorized users cannot gain an initial system foothold by exploiting known weaknesses in internet-facing assets.
Observation	An outside check found the firewall's admin page reachable from the internet at 203.0.113.18. Remote desktop is not exposed.
Evidence reviewed	None linked
Risk	Exposed admin pages are scanned for constantly and are a direct path in when a flaw is announced.
Recommendation	Close the firewall admin page to the internet and manage it only through the IT provider's VPN with MFA.
Owner	IT provider
Target	30 days

F-07 MANAGE CYBERSECURITY OVERSIGHT

CPG goal	1.B Manage Cybersecurity Oversight (CSF 2.0 function: Govern)
Status	In progress
Priority	Medium
CISA rating	Cost Low · Impact High · Ease Moderate
CISA outcome	The organization's cybersecurity risk management strategy, expectations, and policies are established.
Observation	The security policy was approved in March 2026, but it has no yearly review date and the partners have never reviewed security risks or results.
Evidence reviewed	None linked
Risk	Policies fall out of date and security spending is decided without a view of the risks.
Recommendation	Set a yearly policy review date and add a 15-minute security update to the partners' quarterly meeting.
Owner	Managing dentist

F-07 MANAGE CYBERSECURITY OVERSIGHT

Target	60 days
--------	---------

F-08 SUPPLY CHAIN INCIDENT REPORTING & VULNERABILITY DISCLOSURE

CPG goal	1.D Supply Chain Incident Reporting & Vulnerability Disclosure (CSF 2.0 function: Govern)
Status	In progress
Priority	Medium
CISA rating	Cost Moderate · Impact Moderate · Ease Complex
CISA outcome	Organizations more rapidly learn about and respond to known incidents or breaches across vendors and service providers
Observation	Business associate agreements require notice of patient-data breaches. The IT provider's agreement has no duty to report security incidents that do not involve patient data, and software vendors are not asked how they disclose vulnerabilities.
Evidence reviewed	DOC-011 Business associate agreements (9 vendors)
Risk	A breach at the IT provider or a flaw in the practice software could go on for weeks before the practice is told.
Recommendation	Add a 72-hour security incident notice term to the IT provider's agreement at renewal, and subscribe to the practice-management, imaging and phone vendors' security notices.
Owner	Practice administrator
Target	60 days

F-09 MANAGE RISKS FROM MANAGED SERVICE PROVIDERS

CPG goal	1.E Manage Risks from Managed Service Providers (CSF 2.0 function: Govern)
Status	In progress
Priority	Medium
CISA rating	Cost Moderate · Impact Moderate · Ease Complex
CISA outcome	The risks posed by a managed service provider (MSP) are identified, recorded, assessed, prioritized, monitored, and updated over the course of the relationship.
Observation	The IT provider manages every device and has remote access to all of them. Its agreement lists the services, but not the security of its own tools or what it does if it has an incident.
Evidence reviewed	None linked

F-09 MANAGE RISKS FROM MANAGED SERVICE PROVIDERS

Risk	If the IT provider's remote-support tool is compromised, an attacker reaches every device at once.
Recommendation	At renewal, ask the IT provider to confirm MFA on its remote-support tool, 72-hour incident notice and a yearly summary of its own security checks.
Owner	Practice administrator
Target	60 days

F-10 MANAGE ORGANIZATIONAL ASSETS

CPG goal	2.A Manage Organizational Assets (CSF 2.0 function: Identify)
Status	In progress
Priority	Medium
CISA rating	Cost Low · Impact High · Ease Moderate
CISA outcome	A maintained asset inventory to improve cybersecurity resilience by reducing downtime, aiding recovery, bolstering defenses, and improving preparedness.
Observation	The IT provider keeps a device list from its management agent. Two imaging workstations and the phone system were missing, and it is updated only when a device is replaced.
Evidence reviewed	DOC-008 Device and software list (IT provider)
Risk	Unlisted devices miss patches and endpoint protection, and are the first place an attacker hides.
Recommendation	Have the IT provider reconcile the device list each month and add the imaging PCs, phones and network gear.
Owner	IT provider
Target	60 days

F-11 MITIGATE KNOWN VULNERABILITIES

CPG goal	2.B Mitigate Known Vulnerabilities (CSF 2.0 function: Identify)
Status	In progress
Priority	Medium
CISA rating	Cost High · Impact High · Ease Complex
CISA outcome	Reduced likelihood of threat actors exploiting known vulnerabilities to breach organizational networks.
Observation	Windows and third-party patches are applied monthly. The firewall firmware is two releases behind and no vulnerability scan has been run.
Evidence reviewed	DOC-009 Monthly patch compliance reports (IT provider)
Risk	A known firewall flaw is one of the most common ways ransomware groups get in.
Recommendation	Update the firewall now, then run a quarterly external vulnerability scan and fix critical findings within 15 days.
Owner	IT provider
Target	60 days

F-12 OBTAIN INDEPENDENT VALIDATION OF CYBERSECURITY CONTROLS

CPG goal	2.C Obtain Independent Validation of Cybersecurity Controls (CSF 2.0 function: Identify)
Status	Not implemented
Priority	Medium
CISA rating	Cost High · Impact High · Ease Complex
CISA outcome	Validate that implemented security controls are properly configured and working as intended
Observation	No outside test or assessment before this one.
Evidence reviewed	None linked
Risk	Gaps nobody has looked for stay open; the insurer may ask for proof of testing.
Recommendation	Commission an external vulnerability scan this year and an outside test of the Microsoft 365 tenant next year.
Owner	Managing dentist
Target	60 days

F-13 DOCUMENT NETWORK TOPOLOGY

CPG goal	2.E Document Network Topology (CSF 2.0 function: Identify)
Status	Not implemented
Priority	Medium
CISA rating	Cost Low · Impact High · Ease Moderate
CISA outcome	More efficiently and effectively respond to incidents and maintain service continuity.
Observation	No current network diagram.
Evidence reviewed	None linked
Risk	Responders lose hours in an incident working out what connects to what.
Recommendation	Draw a one-page network diagram showing both offices, the imaging server, cloud services and remote access, and review it each year.
Owner	IT provider
Target	60 days

F-14 IMPLEMENT THE PRINCIPLES OF LEAST PRIVILEGE

CPG goal	3.H Implement the Principles of Least Privilege (CSF 2.0 function: Protect)
Status	In progress
Priority	Medium
CISA rating	Cost Low · Impact High · Ease Simple
CISA outcome	Minimizes unauthorized access to systems, data, and processes, reduces human error, and prevents malicious actions; helping ensure the organization's sensitive information and critical assets remain protected.
Observation	PMS roles match each person's job, but every staff account can read the scanned-forms share, and access has not been reviewed this year.
Evidence reviewed	None linked
Risk	Any compromised account exposes far more than that person needs.
Recommendation	Review PMS roles and file-share access every quarter, starting with the scanned-forms share.
Owner	Office manager
Target	60 days

F-15 IMPLEMENT LOGICAL/PHYSICAL NETWORK SEGMENTATION

CPG goal	3.I Implement Logical/Physical Network Segmentation (CSF 2.0 function: Protect)
Status	Not implemented
Priority	Medium
CISA rating	Cost High · Impact High · Ease Complex
CISA outcome	Limiting the impact(s) of a potential breach and preventing adversaries from accessing sensitive data, spaces, and/or critical infrastructure.
Observation	Guest Wi-Fi is separate, but staff PCs, imaging devices, the imaging server and the phones share one flat network.
Evidence reviewed	None linked
Risk	One infected PC can reach the imaging server and every workstation, turning a single click into a practice-wide outage.
Recommendation	Separate the imaging server and devices, staff PCs and phones onto their own networks with firewall rules between them.
Owner	IT provider
Target	90 days

F-16 ENABLE EMAIL SECURITY

CPG goal	3.L Enable Email Security (CSF 2.0 function: Protect)
Status	In progress
Priority	Medium
CISA rating	Cost Low · Impact High · Ease Moderate
CISA outcome	Reduce risk from common email-based threats, such as spoofing, phishing, and interception.
Observation	STARTTLS and SPF are in place. DMARC is set to p=none, so spoofed mail is not blocked.
Evidence reviewed	None linked
Risk	Attackers can send email that appears to come from the practice to patients and vendors.
Recommendation	Confirm DKIM signing, then move DMARC to quarantine and then reject over 60 days.
Owner	IT provider
Target	60 days

F-17 ESTABLISH CHANGE MANAGEMENT PROCESSES

CPG goal	3.N Establish Change Management Processes (CSF 2.0 function: Protect)
Status	Not implemented
Priority	Medium
CISA rating	Cost Moderate · Impact High · Ease Complex
CISA outcome	Policies and procedures exist to manage system changes and configurations.
Observation	Workstations follow a standard build, but the build, the firewall settings and changes to them are not written down.
Evidence reviewed	None linked
Risk	Settings drift over time, unapproved changes go unnoticed, and systems cannot be restored quickly after an incident.
Recommendation	Have the IT provider document the workstation, server and firewall settings and log every change to them.
Owner	IT provider
Target	60 days

F-18 MAINTAIN LOG COLLECTION & STORAGE

CPG goal	3.Q Maintain Log Collection & Storage (CSF 2.0 function: Protect)
Status	Not implemented
Priority	Medium
CISA rating	Cost Moderate · Impact High · Ease Moderate
CISA outcome	Enhance visibility to detect and respond to cyber incidents while ensuring security logs are protected from unauthorized access and tampering.
Observation	Firewall, Microsoft 365 and server logs are kept only where they are made, for default periods, and anyone with admin rights on a device can change them.
Evidence reviewed	None linked
Risk	After an incident there may be no record of what the attacker did, which makes breach scoping slow and costly.
Recommendation	Send firewall, Microsoft 365 and server logs to one place the IT provider monitors, kept at least 90 days, where practice admins cannot change them.
Owner	IT provider

F-18 MAINTAIN LOG COLLECTION & STORAGE

Target	60 days
--------	---------

F-19 PROHIBIT CONNECTION OF UNAUTHORIZED DEVICES

CPG goal	3.R Prohibit Connection of Unauthorized Devices (CSF 2.0 function: Protect)
Status	Scoped
Priority	Medium
CISA rating	Cost Moderate · Impact High · Ease Complex
CISA outcome	Prevent malicious actors from achieving initial access or data exfiltration via unauthorized portable media devices.
Observation	USB storage is allowed on all PCs. The IT provider has quoted a device-control policy for the first quarter.
Evidence reviewed	None linked
Risk	Patient data can leave on a USB stick, and infected drives can bring malware in.
Recommendation	Apply the device-control policy to block USB storage, with an exception for the imaging sensor drivers.
Owner	IT provider
Target	60 days

F-20 IDENTIFY ADVERSE EVENTS

CPG goal	4.B Identify Adverse Events (CSF 2.0 function: Detect)
Status	In progress
Priority	Medium
CISA rating	Cost Moderate · Impact High · Ease Complex
CISA outcome	Organizations can identify adverse security events.
Observation	Endpoint alerts are watched. Microsoft 365 and firewall alerts are not, and there is no written rule for when an alert becomes an incident.
Evidence reviewed	None linked
Risk	Email-based attacks, the most likely threat here, are not detected.
Recommendation	Add Microsoft 365 and firewall alerts to the IT provider's monitoring, with a same-day

F-20 IDENTIFY ADVERSE EVENTS

	response target, and write down when an alert goes to the incident response plan.
Owner	IT provider
Target	60 days

F-21 ESTABLISH INCIDENT COMMUNICATION PROCEDURES

CPG goal	5.A Establish Incident Communication Procedures (CSF 2.0 function: Respond)
Status	Not implemented
Priority	Medium
CISA rating	Cost Low · Impact High · Ease Moderate
CISA outcome	Coordinate crisis communication methods between internal and external organization partners and critical suppliers.
Observation	No plan for who tells staff, patients, vendors or the press what, during an outage or breach.
Evidence reviewed	None linked
Risk	Mixed messages during an incident damage patient trust and can breach notice rules.
Recommendation	Add a one-page communications section to the incident response plan, with draft messages for staff and patients and one named spokesperson.
Owner	Practice administrator
Target	60 days

F-22 ESTABLISH INCIDENT REPORTING PROCEDURES

CPG goal	5.B Establish Incident Reporting Procedures (CSF 2.0 function: Respond)
Status	Not implemented
Priority	Medium
CISA rating	Cost Moderate · Impact High · Ease Moderate
CISA outcome	CISA and other organizations are better able to provide assistance or understand the broader scope of a cyber incident.
Observation	No written steps for reporting an incident to the insurer, law enforcement, HHS or patients.
Evidence reviewed	None linked

F-22 ESTABLISH INCIDENT REPORTING PROCEDURES

Risk	Late notice can void insurance coverage and bring regulatory penalties.
Recommendation	Add a reporting checklist to the incident response plan with contacts and deadlines for the insurer, IC3, HHS and the state.
Owner	Practice administrator
Target	60 days

F-23 INCIDENT PLANNING AND PREPAREDNESS

CPG goal	6.A Incident Planning and Preparedness (CSF 2.0 function: Recover)
Status	Not implemented
Priority	Medium
CISA rating	Cost Moderate · Impact High · Ease Complex
CISA outcome	Organizations are capable of safely and effectively recovering from a cybersecurity incident.
Observation	No restore priorities are written down, and staff have not practised working while systems are down.
Evidence reviewed	None linked
Risk	Recovery drags while the most important systems wait, and the front desk stops when the PMS is unreachable.
Recommendation	Write the order to restore systems (PMS access, imaging server, phones), a paper fallback for the front desk, and a short review after any incident.
Owner	Managing dentist
Target	60 days

F-24 MAINTAIN VULNERABILITY DISCLOSURE/REPORTING PROCESS

CPG goal	2.D Maintain Vulnerability Disclosure/Reporting Process (CSF 2.0 function: Identify)
Status	Scoped
Priority	Low
CISA rating	Cost Low · Impact Low · Ease Moderate
CISA outcome	Organizations more rapidly learn about vulnerabilities or weaknesses.
Observation	No way for outsiders to report a security problem, and no security.txt file. Both are planned for

F-24 MAINTAIN VULNERABILITY DISCLOSURE/REPORTING PROCESS

	the website rebuild in the spring.
Evidence reviewed	None linked
Risk	Low for a practice of this size: a reported flaw may not reach anyone who can act.
Recommendation	Publish a security contact and a security.txt file when the website is rebuilt.
Owner	Office manager
Target	90 days

F-25 ESTABLISH MINIMUM PASSWORD STRENGTH

CPG goal	3.B Establish Minimum Password Strength (CSF 2.0 function: Protect)
Status	In progress
Priority	Low
CISA rating	Cost Low · Impact High · Ease Simple
CISA outcome	Organizational passwords are harder for threat actors to guess or crack.
Observation	Microsoft 365 and the PMS require 14-character passwords. CPG 2.0 asks for 16 or more where the system allows it.
Evidence reviewed	DOC-007 Password and MFA standard (draft)
Risk	Low: 14 characters is strong, but shorter passwords on the imaging PCs are not checked.
Recommendation	Raise the minimum to 16 characters at the next password change and give every staff member the password manager.
Owner	IT provider
Target	90 days

5. 90-DAY ACTION PLAN

The plan sequences the findings so early wins build momentum and later work builds on them. Owners and dates are proposals to confirm with leadership.

DAYS 0–30

Quick wins: high impact, low effort

Action	Finding	Owner
Finish and approve the incident response plan, with the insurer's breach line and the HHS notice steps, and run a one-hour ransomware tabletop exercise with the partners, the office manager and the IT provider before the insurance renewal.	F-01 · 1.C	Practice administrator
Give each staff member their own imaging login and retire the shared accounts.	F-02 · 3.C	Office manager
Turn on Microsoft 365 risky sign-in and failed-login alerts and send them to the IT provider and the practice administrator.	F-03 · 3.E	IT provider
Enforce MFA on every mailbox and on the remote-support tool this month; use number matching or security keys.	F-04 · 3.F	Practice administrator
Limit the scanned-forms share to the front desk and office manager, and move forms into the PMS where possible.	F-05 · 3.K	IT provider
Close the firewall admin page to the internet and manage it only through the IT provider's VPN with MFA.	F-06 · 3.S	IT provider

DAYS 31–60

Foundations: visibility and recovery

Action	Finding	Owner
Set a yearly policy review date and add a 15-minute security update to the partners' quarterly meeting.	F-07 · 1.B	Managing dentist
Add a 72-hour security incident notice term to the IT provider's agreement at renewal, and subscribe to the practice-management, imaging and phone vendors' security notices.	F-08 · 1.D	Practice administrator
At renewal, ask the IT provider to confirm MFA on its remote-support tool, 72-hour incident notice and a yearly summary of its own security checks.	F-09 · 1.E	Practice administrator
Have the IT provider reconcile the device list each month and add the imaging PCs, phones and network gear.	F-10 · 2.A	IT provider
Update the firewall now, then run a quarterly external vulnerability scan and fix critical findings within 15 days.	F-11 · 2.B	IT provider
Commission an external vulnerability scan this year and an outside test of the Microsoft 365 tenant next year.	F-12 · 2.C	Managing dentist
Draw a one-page network diagram showing both offices, the imaging server, cloud services and remote access, and review it each year.	F-13 · 2.E	IT provider

Action	Finding	Owner
Review PMS roles and file-share access every quarter, starting with the scanned-forms share.	F-14 · 3.H	Office manager
Confirm DKIM signing, then move DMARC to quarantine and then reject over 60 days.	F-16 · 3.L	IT provider
Have the IT provider document the workstation, server and firewall settings and log every change to them.	F-17 · 3.N	IT provider
Send firewall, Microsoft 365 and server logs to one place the IT provider monitors, kept at least 90 days, where practice admins cannot change them.	F-18 · 3.Q	IT provider
Apply the device-control policy to block USB storage, with an exception for the imaging sensor drivers.	F-19 · 3.R	IT provider
Add Microsoft 365 and firewall alerts to the IT provider's monitoring, with a same-day response target, and write down when an alert goes to the incident response plan.	F-20 · 4.B	IT provider
Add a one-page communications section to the incident response plan, with draft messages for staff and patients and one named spokesperson.	F-21 · 5.A	Practice administrator
Add a reporting checklist to the incident response plan with contacts and deadlines for the insurer, IC3, HHS and the state.	F-22 · 5.B	Practice administrator
Write the order to restore systems (PMS access, imaging server, phones), a paper fallback for the front desk, and a short review after any incident.	F-23 · 6.A	Managing dentist

DAYS 61–90

Maturity: validate, document, and drill

Action	Finding	Owner
Separate the imaging server and devices, staff PCs and phones onto their own networks with firewall rules between them.	F-15 · 3.I	IT provider
Publish a security contact and a security.txt file when the website is rebuilt.	F-24 · 2.D	Office manager
Raise the minimum to 16 characters at the next password change and give every staff member the password manager.	F-25 · 3.B	IT provider

LONGER TERM

After 90 days, complete network separation and log collection, then commission an outside test and repeat this baseline in April 2027 ahead of a full NIST CSF assessment.

6. 12-MONTH SECURITY ROADMAP

The roadmap groups this assessment's gaps into initiatives, sequenced so high-priority work and foundations come first, and later work builds on them. Timing, owners, and budgets are proposals to confirm with leadership.

	NOV–JAN 27	FEB–APR 27	MAY–JUL 27	AUG–OCT 27	BEYOND 12 MO
Identity & Access	5 ITEMS				
Governance & Leadership	1 ITEM				
Asset & Vulnerability Management	3 ITEMS				
Incident Response		3 ITEMS			
Network & OT Security		3 ITEMS			
Data Protection		1 ITEM			
Backup & Recovery			1 ITEM		
Endpoint, Email & Platform Hardening			3 ITEMS		
Logging & Detection			2 ITEMS		
Third-Party Risk				2 ITEMS	
Assurance & Improvement				1 ITEM	

■ HIGH PRIORITY ■ MEDIUM PRIORITY ■ LOW PRIORITY

QUICK WINS

- 3.C Create Unique Credentials

INITIATIVES

Initiative	Items	Priority	Timing	Owner / budget	Success measure
Identity & Access	3.B, 3.C, 3.E, 3.F, 3.H	High	Nov–Jan 27 to Feb–Apr 27	Practice administrator \$ (under \$5K)	Phishing-resistant MFA on email, remote, and admin access; separate admin accounts; same-day offboarding.
Governance & Leadership	1.B	Medium	Nov–Jan 27	Managing dentist \$ (under \$5K)	Named security owner; approved policies; quarterly leadership risk review held.
Asset & Vulnerability Management	2.A, 2.B, 2.D	Medium	Nov–Jan 27 to Feb–Apr 27	IT provider \$ (under \$5K)	Complete asset inventory reviewed monthly; critical internet-facing vulnerabilities fixed within 14 days.
Incident Response	1.C, 5.A, 5.B	High	Feb–Apr 27 to May–Jul 27	Practice administrator \$ (under \$5K)	Written incident response plan; tabletop exercise in the last 12 months; reporting contacts documented.
Network & OT Security	2.E, 3.I, 3.S	High	Feb–Apr 27 to May–Jul 27	IT provider \$\$ (\$5K–\$25K)	IT and OT separated by a monitored boundary; no OT exposed to the internet; network diagrams current.
Data Protection	3.K	High	Feb–Apr 27	IT provider	Sensitive data mapped; strong encryption in use; no plaintext credentials.
Backup & Recovery	6.A	Medium	May–Jul 27	IT provider	Immutable backups; successful restore test

Initiative	Items	Priority	Timing	Owner / budget	Success measure
				\$ (under \$5K)	in the last 12 months; restore priorities documented.
Endpoint, Email & Platform Hardening	3.L, 3.N, 3.R	Medium	May–Jul 27 to Aug–Oct 27	IT provider \$ (under \$5K)	DMARC at enforcement; macros blocked by default; baseline configurations documented.
Logging & Detection	3.Q, 4.B	Medium	May–Jul 27 to Aug–Oct 27	IT provider \$\$ (\$5K–\$25K)	Critical logs centralized with 90+ days' retention; alerts triaged by a named person or MDR within agreed times.
Third-Party Risk	1.D, 1.E	Medium	Aug–Oct 27 to Beyond 12 mo	Practice administrator	Security and notification clauses in critical vendor contracts; critical suppliers assessed.
Assurance & Improvement	2.C	Medium	Aug–Oct 27	Managing dentist \$ (under \$5K)	Annual independent test; findings tracked to closure.

7. NEXT STEPS

- Review this report with leadership and confirm owners and dates in the action plan.
- Begin the Days 0–30 actions immediately; most require little or no spending.
- Schedule a reassessment in six months to measure progress.
- For board-level reporting, regulatory evidence, or a full risk profile, a NIST CSF 2.0 Risk Assessment builds directly on this baseline.

I'm available to guide your team through implementation, either as advisory hours or through an ongoing vCISO retainer. Your team owns the program; I help them build it right and keep it on course.

Alex Sample, CISSP · hello@example.com · example.com

APPENDIX A. FULL GOAL RESULTS

Goals are listed under the NIST CSF 2.0 function CISA groups them by. Source: CISA, Cybersecurity Performance Goals 2.0.

1. GOVERN

ID	Goal	Status	Finding / evidence / note
1.A	Establish Cybersecurity Responsibilities	Implemented	DOC-001 · Practice administrator named HIPAA security officer in policy v1.2; the IT provider's duties are in its agreement.
1.B	Manage Cybersecurity Oversight	In progress	F-07
1.C	Manage Incident Response Plans	In progress	F-01 · DOC-010
1.D	Supply Chain Incident Reporting & Vulnerability Disclosure	In progress	F-08 · DOC-011
1.E	Manage Risks from Managed Service Providers	In progress	F-09

2. IDENTIFY

ID	Goal	Status	Finding / evidence / note
2.A	Manage Organizational Assets	In progress	F-10 · DOC-008
2.B	Mitigate Known Vulnerabilities	In progress	F-11 · DOC-009
2.C	Obtain Independent Validation of Cybersecurity Controls	Not implemented	F-12
2.D	Maintain Vulnerability Disclosure/Reporting Process	Scoped	F-24
2.E	Document Network Topology	Not implemented	F-13

3. PROTECT

ID	Goal	Status	Finding / evidence / note
3.A	Changing Default Passwords	Implemented	Defaults changed at setup; firewall, Wi-Fi and printers checked on site.
3.B	Establish Minimum Password Strength	In progress	F-25 · DOC-007
3.C	Create Unique Credentials	In progress	F-02
3.D	Revoking Credentials for Departing Staff	Implemented	DOC-002 · Offboarding checklist; both 2026 leavers removed the same day.
3.E	Monitor Unsuccessful (Automated) Login Attempts	In progress	F-03
3.F	Implement Multi-factor Authentication	In progress	F-04 · DOC-007
3.G	Administrators Maintain Separate User and Privileged Accounts	Implemented	Staff are not local admins; IT provider uses separate admin accounts.
3.H	Implement the Principles of Least Privilege	In progress	F-14
3.I	Implement Logical/Physical Network Segmentation	Not implemented	F-15
3.J	Implement Cybersecurity Training	Implemented	DOC-003 · 14 of 14 staff completed 2026 HIPAA and phishing training; new hires before

ID	Goal	Status	Finding / evidence / note
			first login.
3.K	Utilize Strong Encryption	In progress	F-05 · DOC-004
3.L	Enable Email Security	In progress	F-16
3.M	Disable Autorun & Macros By Default	Implemented	Microsoft 365 policy blocks macros in files from the internet; AutoPlay is off by policy.
3.N	Establish Change Management Processes	Not implemented	F-17
3.O	Maintain System Backups & Restoration Ability	Implemented	DOC-005 · Nightly imaging-server backup, offsite copy; restore witnessed Oct 7.
3.P	Maintain Hardware & Software Approval Process	Implemented	DOC-006 · Purchases go through the IT provider; staff cannot install software.
3.Q	Maintain Log Collection & Storage	Not implemented	F-18
3.R	Prohibit Connection of Unauthorized Devices	Scoped	F-19
3.S	Secure Internet Facing Devices	In progress	F-06

4. DETECT

ID	Goal	Status	Finding / evidence / note
4.A	Establish Malicious Code Detection	Implemented	Managed endpoint detection on all 22 endpoints, watched by the IT provider.
4.B	Identify Adverse Events	In progress	F-20

5. RESPOND

ID	Goal	Status	Finding / evidence / note
5.A	Establish Incident Communication Procedures	Not implemented	F-21
5.B	Establish Incident Reporting Procedures	Not implemented	F-22

6. RECOVER

ID	Goal	Status	Finding / evidence / note
6.A	Incident Planning and Preparedness	Not implemented	F-23

APPENDIX B. ABOUT THIS ASSESSMENT

ABOUT THE CISA CPGS

The CPGs 2.0 are voluntary practices with high-impact security actions that outline the highest-priority baseline that measures businesses and critical infrastructure owners of all sizes can take to protect themselves against cyber threats. They were developed based on CISA's operational data, research on the current threat landscape, and collaboration with government, industry groups, and private sector experts to receive input and feedback.

CISA's CPGs are not comprehensive. They do not identify all the cybersecurity practices needed to protect national and economic security and public health and safety. They capture a core set of cybersecurity practices with known risk-reduction value broadly applicable across sectors.

Source: CISA, Cybersecurity Performance Goals 2.0 (CPG 2.0),

<https://www.cisa.gov/cybersecurity-performance-goals-2-0-cpg-2-0>, retrieved October 19, 2026. A work of the U.S. government. CISA groups the goals by NIST CSF 2.0 function; it did not publish a mapping to CSF subcategories, and none is shown in this report.

TOOLS

CISA does not endorse this assessment, this assessor, or any commercial service. The analysis, prioritization, and recommendations in this report are the assessor's own. The assessment is not a certification and does not show compliance with any law, regulation or contract.

ABOUT THE ASSESSOR

Alex Sample is a CISSP-certified security consultant who has led security programs for healthcare practices and professional services firms for twelve years. Example Security Partners serves as the virtual CISO for small and mid-sized organizations.

APPENDIX C. DOCUMENT LIBRARY

The security documents Sample Dental Group (made up) should maintain under the CISA CPG 2.0, the evidence provided during the assessment, and where each document lives. 8 of 35 are in place; 3 need attention; 24 are not yet provided. Files remain in Sample Dental Group (made up)'s own systems, and links for sensitive items are withheld.

Document	Status	Evidence and location	Owner / version / reviewed	CISA CPG 2.0
Information Security Policy	Provided	DOC-001 Information Security Policy v1.2 — SharePoint / OneDrive	Practice administrator, v1.2, 2026-03-10	1.A, 1.B
Security Roles and Responsibilities (RACI)	Not yet provided	—	—	1.A
Risk Management Strategy and Risk Appetite Statement	Not yet provided	—	—	1.B
Risk Assessment and Risk Register	Not yet provided	—	—	2.B
Leadership Security Review Minutes or Metrics Report	Not yet provided	—	—	1.B
Hardware and Software Asset Inventory	Needs review	DOC-008 Device and software list (IT provider) — SharePoint / OneDrive	IT provider, 2025-11-20	2.A, 3.P
Data Inventory and Classification	Not yet provided	—	—	2.A, 3.K
Network Diagram and Data Flows	Not yet provided	—	—	2.E, 3.I
Secure Configuration Baselines	Not yet provided	—	—	3.N, 3.M, 3.A
Vulnerability and Patch Management Procedure, with Recent Scan Results	Provided	DOC-009 Monthly patch compliance reports (IT provider) — SharePoint / OneDrive	IT provider, 2026-10-05	2.B, 3.S
Vulnerability Disclosure Policy and security.txt	Not yet provided	—	—	2.D
Third-Party Security Assessment or Penetration Test Report	Not yet provided	—	—	2.C
Access Control and Account Management Policy	Not yet provided	—	—	3.C, 3.D, 3.G, 3.H
Authentication Standard (Passwords and MFA)	Draft	DOC-007 Password and MFA standard (draft) — SharePoint / OneDrive	Practice administrator, v0.1, 2026-09-12	3.A, 3.B, 3.E, 3.F
Onboarding/Offboarding Checklist and Access Review Records	Provided	DOC-002 Onboarding and offboarding checklist — SharePoint / OneDrive	Practice administrator, v3, 2026-01-15	3.D
Security Awareness Training Records	Provided	DOC-003 2026 HIPAA and phishing training completion report — SharePoint / OneDrive	Practice administrator, 2026-08-29	3.J
OT and Specialized-Role Training Records	Not yet provided	—	—	3.J
Encryption and Key Management	Provided	DOC-004 Device encryption	IT provider,	3.K

Document	Status	Evidence and location	Owner / version / reviewed	CISA CPG 2.0
Standard		compliance report (IT provider) (link withheld)	2026-10-01	
Email Security Configuration (SPF, DKIM, DMARC)	Not yet provided	—	—	3.L
Hardware and Software Approval Process and Allowlist	Provided	DOC-006 IT provider purchasing and software install procedure — SharePoint / OneDrive	IT provider, v2, 2026-05-12	3.P, 3.R
Backup Policy and Restore Test Records	Provided	DOC-005 Backup schedule and quarterly restore test log — SharePoint / OneDrive	IT provider, 2026-09-30	3.O
Business Continuity and Disaster Recovery Plan	Not yet provided	—	—	6.A
Logging and Monitoring Standard (Sources and Retention)	Not yet provided	—	—	3.Q
Alert Triage and Detection Procedure	Not yet provided	—	—	3.E, 4.A, 4.B
Threat Profile (Relevant Threats and Techniques)	Not yet provided	—	—	4.B
Incident Response Plan	Draft	DOC-010 Incident Response Plan (draft) — SharePoint / OneDrive	Practice administrator, v0.3, 2026-09-12	1.C
Tabletop Exercise After-Action Report	Not yet provided	—	—	1.C
Incident Communications and Reporting Procedure	Not yet provided	—	—	5.A, 5.B
Third-Party Risk Management Procedure	Not yet provided	—	—	1.D, 1.E
Critical Vendor and Service Provider Inventory	Not yet provided	—	—	1.E, 1.D
Vendor Contracts with Security and Notification Clauses	Provided	DOC-011 Business associate agreements (9 vendors) (link withheld)	Practice administrator, 2026-06-30	1.D, 1.E
OT Segmentation and Remote Access Standard	Not yet provided	—	—	3.I, 3.S
IT/OT Collaboration Record	Not yet provided	—	—	1.A
Change and Exception Management Procedure	Not yet provided	—	—	3.N
Improvement Tracker or Corrective Action Log	Not yet provided	—	—	2.C