

EXAMPLE SECURITY PARTNERS

NIST CSF 2.0 RISK ASSESSMENT

Current and target profiles · NIST SP 800-30 risk analysis

Prepared for

Sample Dental Group (made up)

Assessment period: September 21, 2026 – October 9, 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

Across the 106 outcomes of the NIST Cybersecurity Framework 2.0, Sample Dental Group (made up) currently averages 1.5 on a 0–5 maturity scale against a target of 2.6. 92 outcomes fall short of target, and the assessment identified 8 risks, 3 of them rated high or very high. Overall risk governance and management practices align with Tier 1 (Partial), with a target of Tier 2 (Risk Informed).

The practice has good habits in the places HIPAA has pushed it: a signed security policy, encrypted devices, monthly patching, managed endpoint protection and tested backups. The gaps are in what holds those habits together: there is no tested plan for an incident or a restore, the network is flat, MFA is incomplete, and nobody reviews the logs or the IT provider's access.

AT A GLANCE

Avg current	Avg target	Outcomes below target	Very high / high risks	Moderate risks	Low / very low risks
1.5	2.6	92	3	3	2

TOP RISKS

ID	Risk	Level	Response	Window
R-01	Ransomware stops patient care and exposes records	Very High	Mitigate	0–90 days
R-02	Business email compromise diverts a payment	High	Mitigate	0–90 days
R-03	IT provider compromise reaches the practice	High	Mitigate	0–90 days
R-04	Breach is not reported on time	Moderate	Mitigate	3–6 months
R-05	Lost or stolen device exposes patient data	Moderate	Mitigate	3–6 months

KEY STRENGTHS

Tested offsite backups, full device encryption, endpoint protection on every device, and 100% staff training.

RECOMMENDED NEXT STEP

Close the three quick wins in the next 30 days: MFA on every mailbox and on the IT provider's remote tool, risky sign-in alerts, and a call-back rule for bank changes. Then approve the incident response plan and run a one-hour tabletop exercise before the cyber insurance renewal in January.

2. SCOPE AND METHODOLOGY

SCOPE

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

Out of scope: The practice-management vendor's own systems, personal devices that do not get practice email, and the building's alarm and HVAC systems.

BUSINESS CONTEXT

Sample Dental Group is a two-office general and pediatric dental practice. Patient scheduling, charting, imaging and claims all depend on the cloud practice-management system and the on-site imaging server. A day without them means about 40 cancelled appointments and roughly \$18,000 in lost production. IT is run by an outside IT provider under a monthly agreement.

APPROACH

The assessment followed the NIST CSF 2.0 Organizational Profile process: define scope, gather information, create Current and Target Profiles, analyze gaps, and build a prioritized action plan. Risks were analyzed using the approach in NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments.

- Interviews with the managing dentist, the practice administrator (HIPAA security officer), the office manager, two front-desk staff and the IT provider's account engineer.
- Review of documentation, including the Information Security Policy, the 2025 HIPAA risk analysis, business associate agreements, training records, backup and restore logs, and the IT provider's patch and endpoint reports.
- Testing and observation: walk-through of both offices, review of Microsoft 365 security settings and MFA coverage, firewall configuration review, and a restore test witnessed on October 7.
- Structured scoring of all 106 CSF 2.0 subcategories, supported by CISA's Cyber Security Evaluation Tool (CSET), followed by independent analysis by the assessor

MATURITY SCALE

Score	Level	Meaning
0	Not performed	The outcome is not achieved.
1	Initial	Achieved ad hoc, dependent on individuals.
2	Repeatable	Performed consistently but informally; limited documentation.
3	Defined	Documented, approved, and applied across the organization.
4	Managed	Measured and monitored, with metrics reviewed by management.
5	Optimized	Continuously improved based on metrics, lessons learned, and threats.

RISK MODEL

Each risk describes a threat event, the vulnerability or condition it exploits, and the resulting likelihood and impact, each rated from Very Low to Very High. The risk level is read from the SP 800-30 likelihood-and-impact matrix below.

LIKELIHOOD	Very High	Very Low	Low	Moderate	High	Very High
	High	Very Low	Low	Moderate	High	Very High
	Moderate	Very Low	Low	Moderate	Moderate	High
	Low	Very Low	Low	Low	Low	Moderate
	Very Low	Very Low	Very Low	Low	Low	Low
		Very Low	Low	Moderate	High	Very High
		IMPACT				

RATING DEFINITIONS

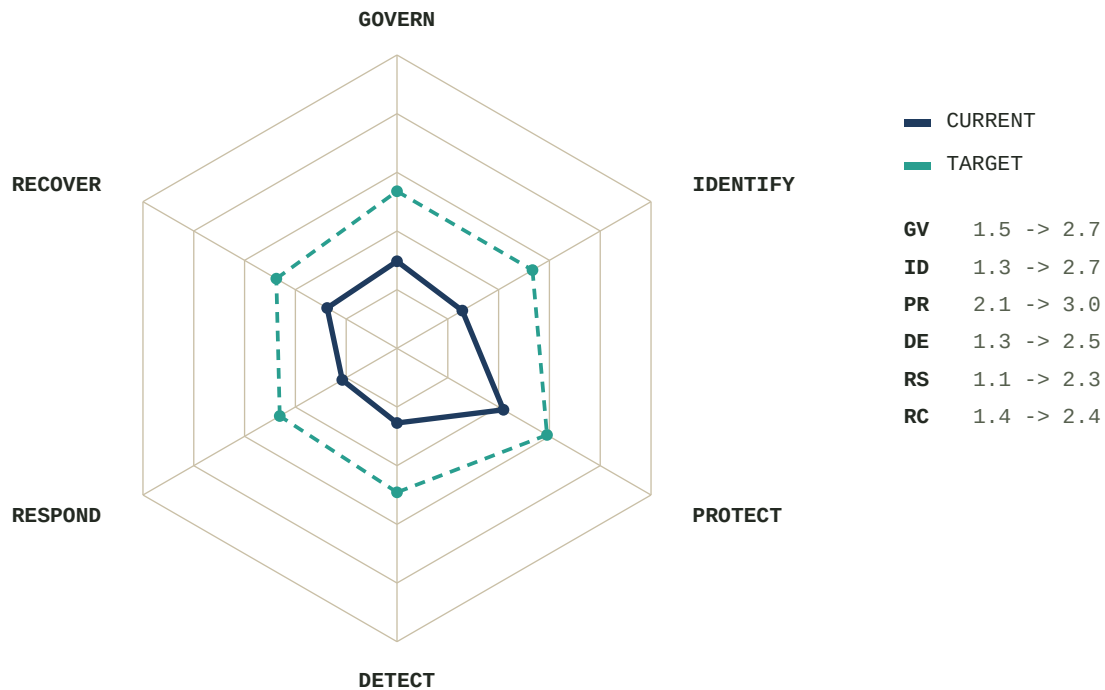
Each subcategory is scored for where the organization is today (current) and where it has chosen to be (target). Target levels reflect the organization's risk and resources; the highest score is not the goal for every item.

Score	Meaning	What the assessor looked for
0 Not performed	The outcome is not being achieved. Nothing is in place.	No practice, tool or document exists. Staff confirm it is not done.
1 Initial	Done sometimes, in reaction to events. It depends on one person's effort and is not written down.	People describe doing it, but there is no record and no consistency from one case to the next.
2 Repeatable	Done regularly and in much the same way each time, but informally. Little or nothing is documented.	Staff describe a consistent routine and some records exist, but there is no approved document.
3 Defined	Written down, approved, communicated and followed across the organization. A named person owns it.	An approved, current document, a named owner, and evidence that practice matches what is written.
4 Managed	Measured and reviewed on a schedule. Leadership sees the results, and exceptions are tracked and corrected.	Metrics or review records over time, leadership reporting, and tracked exceptions with follow-up.
5 Optimized	Improved continuously from lessons learned and changes in threats. Automated where it makes sense.	Records of improvements made from incidents, tests and reviews, and adjustment as threats change.
N/A Not applicable	The outcome does not apply to this environment. It is left out of the scores and averages.	A written reason in the evidence line, for example the technology or activity does not exist here.

LIMITATIONS

This is a point-in-time assessment based on information provided, interviews, and observation during the assessment period. It is not a penetration test or a guarantee against compromise. Risk ratings reflect the assessor's professional judgment and should be revisited as conditions change.

3. CURRENT AND TARGET PROFILE



BY CATEGORY

ID	Category	Current	Target	Gap	Outcomes below target
GV.OC	Organizational Context	2.0	3.0	1.0	4
GV.RM	Risk Management Strategy	1.0	2.4	1.4	7
GV.RR	Roles, Responsibilities, and Authorities	2.0	3.0	1.0	3
GV.PO	Policy	2.5	3.0	0.5	1
GV.OV	Oversight	0.7	2.3	1.7	3
GV.SC	Cybersecurity Supply Chain Risk Management	1.4	2.6	1.2	9
ID.AM	Asset Management	1.6	3.0	1.4	7
ID.RA	Risk Assessment	1.3	2.5	1.2	10
ID.IM	Improvement	0.8	2.5	1.8	4
PR.AA	Identity Management, Authentication, and Access Control	2.2	3.0	0.8	5
PR.AT	Awareness and Training	2.0	3.0	1.0	1
PR.DS	Data Security	2.8	3.0	0.3	1
PR.PS	Platform Security	2.0	3.0	1.0	4

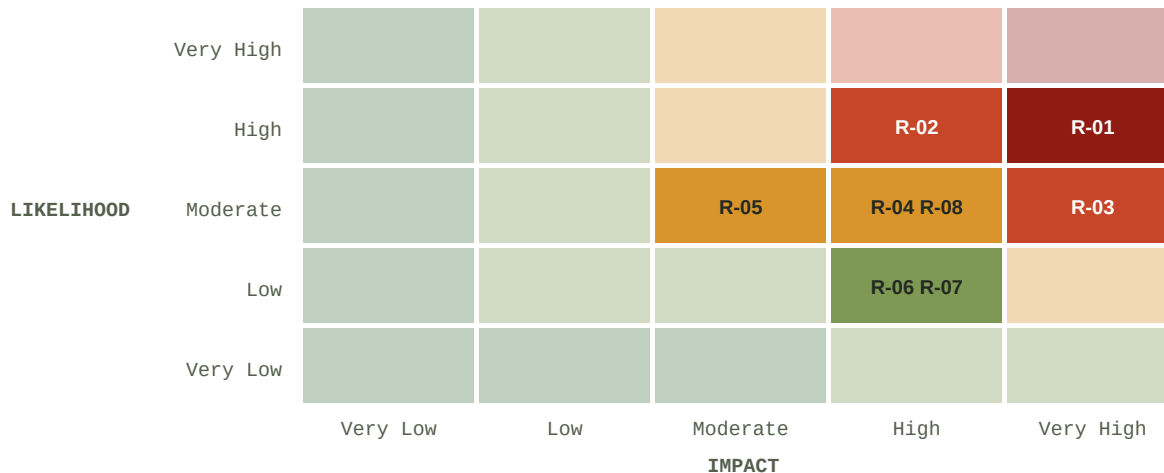
ID	Category	Current	Target	Gap	Outcomes below target
PR . IR	Technology Infrastructure Resilience	1.5	2.8	1.3	4
DE . CM	Continuous Monitoring	1.6	2.6	1.0	3
DE . AE	Adverse Event Analysis	1.0	2.3	1.3	6
RS . MA	Incident Management	1.0	2.4	1.4	5
RS . AN	Incident Analysis	1.0	2.0	1.0	4
RS . CO	Incident Response Reporting and Communication	1.0	2.5	1.5	2
RS . MI	Incident Mitigation	1.5	2.5	1.0	2
RC . RP	Incident Recovery Plan Execution	1.5	2.5	1.0	5
RC . CO	Incident Recovery Communication	1.0	2.0	1.0	2

WHAT THIS MEANS

Govern and Respond are the lowest-scoring functions. Most gaps are one level, closed by writing down and approving what is already partly done. The few two-level gaps (network separation, logging, recovery planning, vendor security) carry most of the ransomware and email-fraud risk.

4. RISK ASSESSMENT

RISK HEAT MAP



RISK REGISTER

ID	Risk	Likelihood	Impact	Level	Response
R-01	Ransomware stops patient care and exposes records	High	Very High	Very High	Mitigate
R-02	Business email compromise diverts a payment	High	High	High	Mitigate
R-03	IT provider compromise reaches the practice	Moderate	Very High	High	Mitigate
R-04	Breach is not reported on time	Moderate	High	Moderate	Mitigate
R-05	Lost or stolen device exposes patient data	Moderate	Moderate	Moderate	Mitigate
R-08	Unpatched firewall is exploited	Moderate	High	Moderate	Mitigate
R-06	Departing staff keep access	Low	High	Low	Mitigate
R-07	Long outage at the cloud practice-management vendor	Low	High	Low	Accept

R-01 RANSOMWARE STOPS PATIENT CARE AND EXPOSES RECORDS

Threat event	A criminal group encrypts the imaging server and workstations and copies patient records first.
Vulnerability / condition	Flat network; no MFA on the IT provider's remote tool; logs not collected; no tested recovery plan.
Related CSF outcomes	PR.IR-01, PR.AA-03, PR.PS-04, RC.RP-01
Likelihood · Impact	High · Very High
Risk level	Very High

R-01 RANSOMWARE STOPS PATIENT CARE AND EXPOSES RECORDS

Response	Mitigate
Recommendation	Put MFA on every remote path, separate imaging and staff networks, and write and test a recovery plan.
Owner	Practice administrator with IT provider
Roadmap window	0–90 days

R-02 BUSINESS EMAIL COMPROMISE DIVERTS A PAYMENT

Threat event	An attacker takes over a staff mailbox and changes a vendor's bank details.
Vulnerability / condition	MFA missing on 3 of 14 mailboxes; no call-back rule for bank changes; sign-in alerts off.
Related CSF outcomes	PR.AA-03, DE.CM-03
Likelihood · Impact	High · High
Risk level	High
Response	Mitigate
Recommendation	Enforce MFA on all mailboxes, turn on risky sign-in alerts, and require a call-back and two approvers for bank changes.
Owner	Practice administrator
Roadmap window	0–90 days

R-03 IT PROVIDER COMPROMISE REACHES THE PRACTICE

Threat event	An attacker who breaches the IT provider uses its remote tool to reach every device.
Vulnerability / condition	Remote tool without MFA; remote sessions not logged; no security terms in the IT contract.
Related CSF outcomes	GV.SC-06, GV.SC-05, DE.CM-06
Likelihood · Impact	Moderate · Very High
Risk level	High
Response	Mitigate
Recommendation	Require MFA and session logging on the remote tool, and add security and notice terms at the contract renewal.
Owner	Managing dentist

R-03 IT PROVIDER COMPROMISE REACHES THE PRACTICE

Roadmap window	0–90 days
----------------	-----------

R-04 BREACH IS NOT REPORTED ON TIME

Threat event	A breach is found, but HHS, patients and the insurer are notified late.
Vulnerability / condition	Incident response plan in draft; no notice procedure; breach coach not contacted.
Related CSF outcomes	RS.MA-01, RS.CO-02
Likelihood · Impact	Moderate · High
Risk level	Moderate
Response	Mitigate
Recommendation	Approve the incident response plan with a notice checklist and the insurer's breach line, and rehearse it once a year.
Owner	Practice administrator
Roadmap window	3–6 months

R-05 LOST OR STOLEN DEVICE EXPOSES PATIENT DATA

Threat event	A laptop or phone with access to patient records is lost or stolen.
Vulnerability / condition	Laptops encrypted; staff phones with email are not managed.
Related CSF outcomes	PR.DS-01, PR.AA-05
Likelihood · Impact	Moderate · Moderate
Risk level	Moderate
Response	Mitigate
Recommendation	Enroll staff phones that get email in device management, with remote wipe.
Owner	IT provider
Roadmap window	3–6 months

R-08 UNPATCHED FIREWALL IS EXPLOITED

Threat event	An attacker uses a known firewall flaw to get onto the network.
Vulnerability / condition	Firewall firmware two releases behind; no vulnerability scanning.
Related CSF outcomes	PR.PS-03, ID.RA-01
Likelihood · Impact	Moderate · High
Risk level	Moderate
Response	Mitigate
Recommendation	Update the firewall now and add quarterly external vulnerability scans.
Owner	IT provider
Roadmap window	3–6 months

R-06 DEPARTING STAFF KEEP ACCESS

Threat event	A former employee still signs in to the PMS or email.
Vulnerability / condition	Offboarding checklist used, but no periodic access review; shared front-desk logins.
Related CSF outcomes	PR.AA-01, PR.AA-05
Likelihood · Impact	Low · High
Risk level	Low
Response	Mitigate
Recommendation	Replace shared logins and review PMS and email access each quarter.
Owner	Practice administrator
Roadmap window	6–12 months

R-07 LONG OUTAGE AT THE CLOUD PRACTICE-MANAGEMENT VENDOR

Threat event	The PMS vendor has an outage of several days.
Vulnerability / condition	No downtime procedure for scheduling and charting.
Related CSF outcomes	GV.OC-05, RC.RP-01
Likelihood · Impact	Low · High
Risk level	Low
Response	Accept
Recommendation	Keep a printed day sheet and a downtime procedure; accept the residual risk.
Owner	Office manager
Roadmap window	6–12 months

5. ROADMAP

Actions are sequenced by risk level so the highest risks are addressed first. Owners and dates are proposals to confirm with leadership.

0–90 DAYS

Action	Risk	Level	Owner
Put MFA on every remote path, separate imaging and staff networks, and write and test a recovery plan.	R-01	Very High	Practice administrator with IT provider
Enforce MFA on all mailboxes, turn on risky sign-in alerts, and require a call-back and two approvers for bank changes.	R-02	High	Practice administrator
Require MFA and session logging on the remote tool, and add security and notice terms at the contract renewal.	R-03	High	Managing dentist

3–6 MONTHS

Action	Risk	Level	Owner
Approve the incident response plan with a notice checklist and the insurer's breach line, and rehearse it once a year.	R-04	Moderate	Practice administrator
Enroll staff phones that get email in device management, with remote wipe.	R-05	Moderate	IT provider
Update the firewall now and add quarterly external vulnerability scans.	R-08	Moderate	IT provider

6–12 MONTHS

Action	Risk	Level	Owner
Replace shared logins and review PMS and email access each quarter.	R-06	Low	Practice administrator

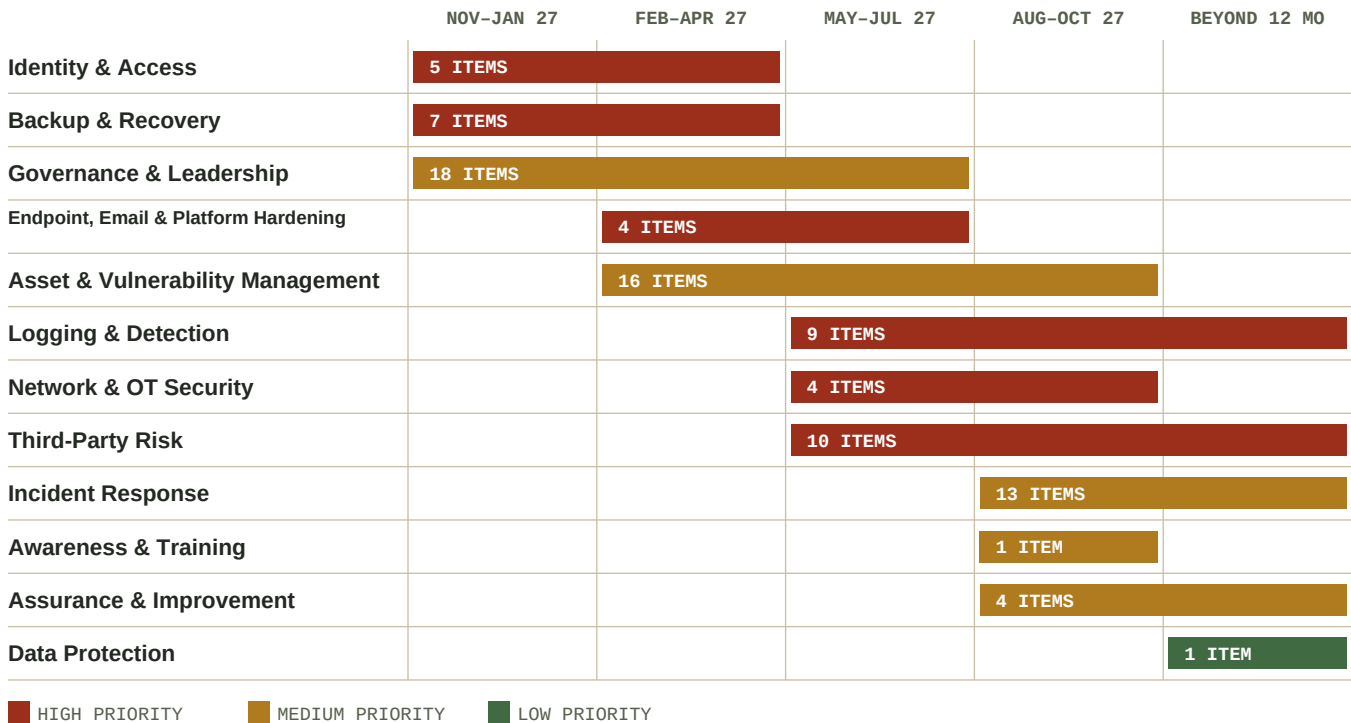
ACCEPTED RISKS

Leadership should formally acknowledge these risks and revisit them at the next assessment:

- R-07 Long outage at the cloud practice-management vendor (Low)

6. INITIATIVE ROADMAP (12 MONTHS)

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.



QUICK WINS

- PR.AA-03 Users, services, and hardware are authenticated
- DE.CM-06 External service provider activities and services are monitored to find potentially adverse events

INITIATIVES

Initiative	Items	Priority	Timing	Owner / budget	Success measure
Identity & Access	PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-04, PR.AA-05	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.
Backup & Recovery	RC.RP-01, RC.RP-02, RC.RP-04, RC.RP-05, RC.RP-06, RC.CO-03, RC.CO-04	High	Nov–Jan 27 to Feb–Apr 27	IT provider \$ (under \$5K)	Immutable backups; successful restore test in the last 12 months; restore priorities documented.
Governance & Leadership	GV.OC-01, GV.OC-02, GV.OC-04, GV.OC-05, GV.RM-01, GV.RM-02,	Medium	Nov–Jan 27 to May–Jul 27	Managing dentist \$ (under \$5K)	Named security owner; approved policies; quarterly leadership risk review held.

Initiative	Items	Priority	Timing	Owner / budget	Success measure
	GV.RM-03, GV.RM-04, GV.RM-05, GV.RM-06, GV.RM-07, GV.RR-01, GV.RR-02, GV.RR-03, GV.PO-02, GV.OV-01, GV.OV-02, GV.OV-03				
Endpoint, Email & Platform Hardening	PR.PS-01, PR.PS-03, PR.PS-04, PR.PS-05	High	Feb–Apr 27 to May–Jul 27	IT provider \$ (under \$5K)	DMARC at enforcement; macros blocked by default; baseline configurations documented.
Asset & Vulnerability Management	ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-04, ID.AM-05, ID.AM-07, ID.AM-08, ID.RA-01, ID.RA-02, ID.RA-03, ID.RA-04, ID.RA-05, ID.RA-06, ID.RA-07, ID.RA-08, ID.RA-09	Medium	Feb–Apr 27 to Aug–Oct 27	IT provider \$ (under \$5K)	Complete asset inventory reviewed monthly; critical internet-facing vulnerabilities fixed within 14 days.
Logging & Detection	DE.CM-01, DE.CM-03, DE.CM-06, DE.AE-02, DE.AE-03, DE.AE-04, DE.AE-06, DE.AE-07, DE.AE-08	High	May–Jul 27 to Beyond 12 mo	IT provider \$\$ (\$5K–\$25K)	Critical logs centralized with 90+ days' retention; alerts triaged by a named person or MDR within agreed times.
Network & OT Security	PR.IR-01, PR.IR-02, PR.IR-03, PR.IR-04	High	May–Jul 27 to Aug–Oct 27	IT provider \$\$ (\$5K–\$25K)	IT and OT separated by a monitored boundary; no OT exposed to the internet; network diagrams current.
Third-Party Risk	GV.SC-01, GV.SC-02, GV.SC-03, GV.SC-04, GV.SC-06, GV.SC-07, GV.SC-08, GV.SC-09, GV.SC-10, ID.RA-10	High	May–Jul 27 to Beyond 12 mo	Practice administrator	Security and notification clauses in critical vendor contracts; critical suppliers assessed.
Incident Response	RS.MA-01, RS.MA-02, RS.MA-03, RS.MA-04, RS.MA-05, RS.AN-03, RS.AN-06, RS.AN-07, RS.AN-08, RS.CO-02,	Medium	Aug–Oct 27 to Beyond 12 mo	Practice administrator \$ (under \$5K)	Written incident response plan; tabletop exercise in the last 12 months; reporting contacts documented.

Initiative	Items	Priority	Timing	Owner / budget	Success measure
	RS.CO-03, RS.MI-01, RS.MI-02				
Awareness & Training	PR.AT-02	Medium	Aug–Oct 27	Office manager \$ (under \$5K)	Annual training completed by all staff; phishing-simulation results improving.
Assurance & Improvement	ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	Medium	Aug–Oct 27 to Beyond 12 mo	Managing dentist \$ (under \$5K)	Annual independent test; findings tracked to closure.
Data Protection	PR.DS-10	Low	Beyond 12 mo	IT provider	Sensitive data mapped; strong encryption in use; no plaintext credentials.

7. NEXT STEPS

- Review this report with leadership and confirm risk owners, responses, and roadmap dates.
- Record formal acceptance for any risk leadership chooses not to treat.
- Track roadmap progress monthly and update the Current Profile quarterly.
- Reassess annually, or after a major incident, acquisition, or technology change.

I'm available to guide your team through the roadmap, 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 PROFILE

Current and target scores for every CSF 2.0 subcategory, with the assessor's evidence notes.

GOVERN (GV)

ID	Outcome	Cur	Tgt	Evidence / note
GV.OC-01	The organizational mission is understood and informs cybersecurity risk management	2	3	Mission (patient care, 2 offices) understood by the partners; not tied to a security plan.
GV.OC-02	Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	2	3	Patients, payers, the IT provider and the landlord's expectations known informally.
GV.OC-03	Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed	3	3	DOC-001 · HIPAA Security Rule and state breach-notice duties tracked in the security policy.
GV.OC-04	Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated	1	3	No written list of the services patients rely on (scheduling, imaging, e-prescribing).
GV.OC-05	Outcomes, capabilities, and services that the organization depends on are understood and communicated	2	3	Depends on the cloud practice-management system (PMS), the IT provider and the claims clearinghouse; known, not written.
GV.RM-01	Risk management objectives are established and agreed to by organizational stakeholders	1	3	No agreed security risk objectives.
GV.RM-02	Risk appetite and risk tolerance statements are established, communicated, and maintained	0	2	No risk appetite or tolerance statement.
GV.RM-03	Cybersecurity risk management activities and outcomes are included in enterprise risk management processes	1	2	Security risk reaches partner meetings only after an incident.
GV.RM-04	Strategic direction that describes appropriate risk response options is established and communicated	1	2	
GV.RM-05	Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	1	3	No set way for the IT provider to raise risks to the partners.
GV.RM-06	A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated	2	3	DOC-010 · 2025 HIPAA risk analysis used a standard template; not updated since.
GV.RM-07	Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions	1	2	
GV.RR-01	Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving	2	3	Managing dentist sponsors security; no regular review of it.
GV.RR-02	Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced	2	3	DOC-001 · Practice administrator is the named HIPAA security officer; duties not written down.
GV.RR-03	Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies	1	3	No security budget line; spending is decided case by case with the IT provider.
GV.RR-04	Cybersecurity is included in human resources practices	3	3	DOC-002 · Onboarding includes HIPAA acknowledgment and background check; offboarding checklist used.
GV.PO-01	Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced	3	3	DOC-001 · Information Security Policy v1.2 approved March 2026 and signed by all 14 staff.
GV.PO-02	Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission	2	3	DOC-001 · Annual review set in the policy; first review due March 2027.
GV.OV-01	Cybersecurity risk management strategy outcomes are reviewed to	1	3	

ID	Outcome	Cur	Tgt	Evidence / note
	inform and adjust strategy and direction			
GV.OV-02	The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks	1	2	
GV.OV-03	Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed	0	2	No security measures reported to the partners.
GV.SC-01	A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders	1	3	No supplier risk program.
GV.SC-02	Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally	2	3	IT provider and software vendors' security roles known; not written.
GV.SC-03	Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes	1	2	
GV.SC-04	Suppliers are known and prioritized by criticality	2	3	Vendor list kept in the accounting system; not ranked by how critical each is.
GV.SC-05	Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties	3	3	DOC-003 · Business associate agreements on file for every vendor that handles patient data.
GV.SC-06	Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships	1	3	No security questions asked before signing a new vendor.
GV.SC-07	The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship	1	2	
GV.SC-08	Relevant suppliers and other third parties are included in incident planning, response, and recovery activities	1	3	Vendors are not part of incident planning.
GV.SC-09	Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle	1	2	
GV.SC-10	Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement	1	2	

IDENTIFY (ID)

ID	Outcome	Cur	Tgt	Evidence / note
ID.AM-01	Inventories of hardware managed by the organization are maintained	2	3	DOC-011 · IT provider keeps a device list; two imaging workstations were missing from it.
ID.AM-02	Inventories of software, services, and systems managed by the organization are maintained	2	3	DOC-011 · Software list from the IT provider's management agent; not reviewed by the practice.
ID.AM-03	Representations of the organization's authorized network communication and internal and external network data flows are maintained	1	3	No current network diagram; flows to the imaging server and cloud PMS undocumented.
ID.AM-04	Inventories of services provided by suppliers are maintained	2	3	Cloud services known (PMS, email, clearinghouse, phones); list incomplete.
ID.AM-05	Assets are prioritized based on classification, criticality, resources, and impact on the mission	1	3	Systems not ranked by how critical they are to patient care.
ID.AM-07	Inventories of data and corresponding metadata for designated data types are maintained	1	3	Patient data locations known informally: PMS, imaging server, scanned-forms share.
ID.AM-08	Systems, hardware, software, services, and data are managed throughout their life cycles	2	3	DOC-011 · Devices replaced on a 5-year cycle; drive disposal certificates kept.
ID.RA-01	Vulnerabilities in assets are identified, validated, and recorded	2	3	DOC-007 · Monthly patch reports from the IT

ID	Outcome	Cur	Tgt	Evidence / note
				provider; no vulnerability scanning.
ID . RA - 02	Cyber threat intelligence is received from information sharing forums and sources	1	2	No threat information sources; relies on the IT provider.
ID . RA - 03	Internal and external threats to the organization are identified and recorded	1	2	
ID . RA - 04	Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded	2	3	DOC-010 · 2025 risk analysis rated likelihood and impact for 12 threats.
ID . RA - 05	Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization	2	3	DOC-010
ID . RA - 06	Risk responses are chosen, prioritized, planned, tracked, and communicated	1	3	Risk responses not tracked to completion.
ID . RA - 07	Changes and exceptions are managed, assessed for risk impact, recorded, and tracked	1	2	Changes made by the IT provider without a written change record.
ID . RA - 08	Processes for receiving, analyzing, and responding to vulnerability disclosures are established	0	2	No way for outsiders to report a vulnerability.
ID . RA - 09	The authenticity and integrity of hardware and software are assessed prior to acquisition and use	2	3	Hardware and software purchases go through the IT provider.
ID . RA - 10	Critical suppliers are assessed prior to acquisition	1	2	
ID . IM - 01	Improvements are identified from evaluations	1	3	
ID . IM - 02	Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties	0	2	No tabletop exercise or outside test to date.
ID . IM - 03	Improvements are identified from execution of operational processes, procedures, and activities	1	2	
ID . IM - 04	Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved	1	3	Incident response plan in draft.

PROTECT (PR)

ID	Outcome	Cur	Tgt	Evidence / note
PR . AA - 01	Identities and credentials for authorized users, services, and hardware are managed by the organization	2	3	Named accounts in Microsoft 365 and the PMS; two shared front-desk logins on imaging PCs.
PR . AA - 02	Identities are proofed and bound to credentials based on the context of interactions	2	3	
PR . AA - 03	Users, services, and hardware are authenticated	2	3	DOC-013 · MFA on email for 11 of 14 staff; none on the PMS or the IT provider's remote tool.
PR . AA - 04	Identity assertions are protected, conveyed, and verified	2	3	
PR . AA - 05	Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	2	3	DOC-002 · PMS access granted by role; no periodic access review.
PR . AA - 06	Physical access to assets is managed, monitored, and enforced commensurate with risk	3	3	DOC-005 · Server closet locked; monitored alarm; visitors signed in at the front desk.
PR . AT - 01	Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind	3	3	DOC-004 · Annual HIPAA and phishing training completed by 14 of 14 staff (records on file).
PR . AT - 02	Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind	1	3	Practice administrator has no role-specific security training.
PR . DS - 01	The confidentiality, integrity, and availability of data-at-rest are protected	3	3	DOC-006 · BitLocker on all laptops and workstations; IT provider's compliance report reviewed.

ID	Outcome	Cur	Tgt	Evidence / note
PR.DS-02	The confidentiality, integrity, and availability of data-in-transit are protected	3	3	DOC-006 · TLS on email and the PMS; patient email goes through the encrypted portal.
PR.DS-10	The confidentiality, integrity, and availability of data-in-use are protected	2	3	
PR.DS-11	Backups of data are created, protected, maintained, and tested	3	3	DOC-008 · Nightly backup of the imaging server with an offsite copy; quarterly restore tests on file.
PR.PS-01	Configuration management practices are established and applied	2	3	Workstation build is standard but not written down.
PR.PS-02	Software is maintained, replaced, and removed commensurate with risk	3	3	DOC-007 · Windows and third-party patches applied monthly by the IT provider; reports on file.
PR.PS-03	Hardware is maintained, replaced, and removed commensurate with risk	2	3	Firewall firmware two releases behind.
PR.PS-04	Log records are generated and made available for continuous monitoring	1	3	Logs kept only on each device, for default periods.
PR.PS-05	Installation and execution of unauthorized software are prevented	2	3	Staff cannot install software; exceptions handled by the IT provider.
PR.PS-06	Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle	N/A	—	No software is developed in-house.
PR.IR-01	Networks and environments are protected from unauthorized logical access and usage	1	3	Guest Wi-Fi is separate; imaging devices, PCs and phones share one flat network.
PR.IR-02	The organization's technology assets are protected from environmental threats	2	3	DOC-005 · Server closet on a UPS; no temperature monitoring.
PR.IR-03	Mechanisms are implemented to achieve resilience requirements in normal and adverse situations	1	2	
PR.IR-04	Adequate resource capacity to ensure availability is maintained	2	3	

DETECT (DE)

ID	Outcome	Cur	Tgt	Evidence / note
DE.CM-01	Networks and network services are monitored to find potentially adverse events	1	3	Firewall alerts go to a shared mailbox at the IT provider; not reviewed daily.
DE.CM-02	The physical environment is monitored to find potentially adverse events	2	2	Office alarm monitored by the alarm company.
DE.CM-03	Personnel activity and technology usage are monitored to find potentially adverse events	1	3	Microsoft 365 risky sign-in alerts not turned on.
DE.CM-06	External service provider activities and services are monitored to find potentially adverse events	1	2	The IT provider's remote sessions are not logged or reviewed by the practice.
DE.CM-09	Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	3	3	DOC-009 · Managed endpoint detection and response on all 22 endpoints, watched by the IT provider.
DE.AE-02	Potentially adverse events are analyzed to better understand associated activities	1	3	
DE.AE-03	Information is correlated from multiple sources	1	2	
DE.AE-04	The estimated impact and scope of adverse events are understood	1	2	
DE.AE-06	Information on adverse events is provided to authorized staff and tools	2	3	IT provider phones the practice administrator about endpoint alerts.
DE.AE-07	Cyber threat intelligence and other contextual information are integrated into the analysis	0	2	
DE.AE-08	Incidents are declared when adverse events meet the defined incident criteria	1	2	

RESPOND (RS)

ID	Outcome	Cur	Tgt	Evidence / note
RS.MA-01	The incident response plan is executed in coordination with relevant third parties once an incident is declared	1	3	DOC-012 · Incident response plan drafted with the IT provider; not approved or tested.
RS.MA-02	Incident reports are triaged and validated	1	3	
RS.MA-03	Incidents are categorized and prioritized	1	2	
RS.MA-04	Incidents are escalated or elevated as needed	1	2	
RS.MA-05	The criteria for initiating incident recovery are applied	1	2	
RS.AN-03	Analysis is performed to establish what has taken place during an incident and the root cause of the incident	1	2	No agreed forensic support; the cyber policy's breach panel has not been contacted.
RS.AN-06	Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved	1	2	
RS.AN-07	Incident data and metadata are collected, and their integrity and provenance are preserved	1	2	
RS.AN-08	An incident's magnitude is estimated and validated	1	2	
RS.CO-02	Internal and external stakeholders are notified of incidents	1	3	Breach-notice duties (HHS, patients, state) understood; no written procedure.
RS.CO-03	Information is shared with designated internal and external stakeholders	1	2	
RS.MI-01	Incidents are contained	2	3	Endpoint tool can isolate a device automatically.
RS.MI-02	Incidents are eradicated	1	2	

RECOVER (RC)

ID	Outcome	Cur	Tgt	Evidence / note
RC.RP-01	The recovery portion of the incident response plan is executed once initiated from the incident response process	1	3	No written recovery plan; restore steps known only to the IT provider.
RC.RP-02	Recovery actions are selected, scoped, prioritized, and performed	1	2	
RC.RP-03	The integrity of backups and other restoration assets is verified before using them for restoration	3	3	DOC-008 · Quarterly restore tests confirm backup integrity.
RC.RP-04	Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms	1	2	
RC.RP-05	The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed	2	3	
RC.RP-06	The end of incident recovery is declared based on criteria, and incident-related documentation is completed	1	2	
RC.CO-03	Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders	1	2	
RC.CO-04	Public updates on incident recovery are shared using approved methods and messaging	1	2	

APPENDIX B. ABOUT THIS ASSESSMENT

ABOUT NIST CSF 2.0

The NIST Cybersecurity Framework 2.0 (NIST CSWP 29, February 2024) is a taxonomy of 106 high-level cybersecurity outcomes organized into six Functions — Govern, Identify, Protect, Detect, Respond, and Recover — and 22 Categories. It is voluntary, sector-neutral, and widely used to understand, assess, prioritize, and communicate cybersecurity risk.

CSF TIERS

Tier	Description
1 Partial	Risk strategy applied ad hoc; limited organizational awareness of cybersecurity risk.
2 Risk Informed	Practices approved by management but not organization-wide policy; awareness exists.
3 Repeatable	Practices formally approved as policy, applied consistently, and reviewed.
4 Adaptive	Practices adapt continuously based on lessons learned and predictive indicators.

TOOLS

Structured scoring was supported by CISA's Cyber Security Evaluation Tool (CSET). NIST and CISA do not endorse this assessment, this assessor, or any commercial service. The analysis, risk ratings, and recommendations in this report are the assessor's own.

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 NIST CSF 2.0, the evidence provided during the assessment, and where each document lives. 9 of 35 are in place; 4 need attention; 22 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	NIST CSF 2.0
Information Security Policy	Provided	DOC-001 Information Security Policy v1.2 — SharePoint / OneDrive	Practice administrator, v1.2, 2026-03-10	GV.PO-01, GV.PO-02, GV.OC-03, GV.RR-02
Security Roles and Responsibilities (RACI)	Not yet provided	—	—	GV.RR-01, GV.RR-02, GV.RR-03
Risk Management Strategy and Risk Appetite Statement	Not yet provided	—	—	GV.RM-01, GV.RM-02, GV.RM-03, GV.RM-04, GV.RM-05, GV.RM-07, GV.OC-01, GV.OC-02, GV.OC-04, GV.OC-05
Risk Assessment and Risk Register	Needs review	DOC-010 2025 HIPAA security risk analysis — SharePoint / OneDrive	Practice administrator, v2025, 2025-04-18	GV.RM-06, ID.RA-04, ID.RA-05, ID.RA-06
Leadership Security Review Minutes or Metrics Report	Not yet provided	—	—	GV.OV-01, GV.OV-02, GV.OV-03, GV.RR-01
Hardware and Software Asset Inventory	Needs review	DOC-011 Device and software list (IT provider) — SharePoint / OneDrive	IT provider, 2025-11-20	ID.AM-01, ID.AM-02, ID.AM-05, ID.AM-08
Data Inventory and Classification	Not yet provided	—	—	ID.AM-07, PR.DS-01
Network Diagram and Data Flows	Not yet provided	—	—	ID.AM-03, PR.IR-01
Secure Configuration Baselines	Not yet provided	—	—	PR.PS-01
Vulnerability and Patch Management Procedure, with Recent Scan Results	Provided	DOC-007 Monthly patch compliance reports (IT provider) — SharePoint / OneDrive	IT provider, 2026-10-05	ID.RA-01, PR.PS-02, PR.PS-03
Vulnerability Disclosure Policy and security.txt	Not yet provided	—	—	ID.RA-08
Third-Party Security Assessment or Penetration Test Report	Not yet provided	—	—	ID.IM-01, ID.IM-02
Access Control and Account Management Policy	Not yet provided	—	—	PR.AA-01, PR.AA-02, PR.AA-05
Authentication Standard (Passwords and MFA)	Draft	DOC-013 Password and MFA standard (draft) — SharePoint / OneDrive	Practice administrator, v0.1, 2026-09-12	PR.AA-03, PR.AA-04
Onboarding/Offboarding Checklist and Access Review Records	Provided	DOC-002 Onboarding and offboarding checklist — SharePoint / OneDrive	Practice administrator, v3, 2026-01-15	PR.AA-05, GV.RR-04
Physical and Environmental Security Procedure	Provided	DOC-005 Office security and visitor procedure — SharePoint / OneDrive	Practice administrator, v1.0, 2026-02-02	PR.AA-06, PR.IR-02, DE.CM-02

Document	Status	Evidence and location	Owner / version / reviewed	NIST CSF 2.0
Security Awareness Training Records	Provided	DOC-004 2026 HIPAA and phishing training completion report — SharePoint / OneDrive	Practice administrator, 2026-08-29	PR.AT-01
OT and Specialized-Role Training Records	Not yet provided	—	—	PR.AT-02
Encryption and Key Management Standard	Provided	DOC-006 Device encryption compliance report (IT provider) (link withheld)	IT provider, 2026-10-01	PR.DS-01, PR.DS-02, PR.DS-10
Email Security Configuration (SPF, DKIM, DMARC)	Not yet provided	—	—	PR.PS-01
Hardware and Software Approval Process and Allowlist	Not yet provided	—	—	PR.PS-05, ID.RA-09
Backup Policy and Restore Test Records	Provided	DOC-008 Backup schedule and quarterly restore test log — SharePoint / OneDrive	IT provider, 2026-09-30	PR.DS-11, RC.RP-03
Business Continuity and Disaster Recovery Plan	Not yet provided	—	—	PR.IR-03, PR.IR-04, RC.RP-01, RC.RP-02, RC.RP-04, RC.RP-05, RC.RP-06
Logging and Monitoring Standard (Sources and Retention)	Provided	DOC-009 Endpoint detection and response coverage report (link withheld)	IT provider, 2026-10-02	PR.PS-04, DE.CM-01, DE.CM-03, DE.CM-09
Alert Triage and Detection Procedure	Not yet provided	—	—	DE.AE-02, DE.AE-03, DE.AE-04, DE.AE-06, DE.AE-08
Threat Profile (Relevant Threats and Techniques)	Not yet provided	—	—	ID.RA-02, ID.RA-03, DE.AE-07
Incident Response Plan	Draft	DOC-012 Incident Response Plan (draft) — SharePoint / OneDrive	Practice administrator, v0.3, 2026-09-12	RS.MA-01, RS.MA-02, RS.MA-03, RS.MA-04, RS.MA-05, RS.AN-03, RS.AN-06, RS.AN-07, RS.AN-08, RS.MI-01, RS.MI-02, ID.IM-04
Tabletop Exercise After-Action Report	Not yet provided	—	—	ID.IM-02, ID.IM-04
Incident Communications and Reporting Procedure	Not yet provided	—	—	RS.CO-02, RS.CO-03, RC.CO-03, RC.CO-04
Third-Party Risk Management Procedure	Not yet provided	—	—	GV.SC-01, GV.SC-02, GV.SC-03, GV.SC-06, GV.SC-07, GV.SC-09, GV.SC-10, ID.RA-10
Critical Vendor and Service Provider Inventory	Not yet provided	—	—	GV.SC-04, ID.AM-04, DE.CM-06
Vendor Contracts with Security and Notification Clauses	Provided	DOC-003 Business associate agreements (9 vendors) (link withheld)	Practice administrator, 2026-06-30	GV.SC-05, GV.SC-08
OT Segmentation and Remote Access Standard	Not yet provided	—	—	PR.IR-01
Change and Exception Management Procedure	Not yet provided	—	—	ID.RA-07
Improvement Tracker or Corrective Action Log	Not yet provided	—	—	ID.IM-01, ID.IM-03, GV.OV-03