Fall, 2025

Designing an Information Security Policy and Compliance Plan for a Dental Clinic: A NIST Cybersecurity Framework Approach to Managing ePHI Risks

Team/Students: ISEC 695-1 / Tomas Heredia & Mauricio Bisogno | Business Advisor: James Adams | Professor: Dr. Yair Levy, Professor of IS & Cybersecurity

INTRODUCTION

Healthcare delivery is increasingly dependent on interconnected digital systems and electronic protected health information (ePHI), which elevates cybersecurity and compliance risks for outpatient clinics such as dental practices (Bastidas, 2020). The Health Insurance Portability and Accountability Act (HIPAA) Security Rule (2024) establishes national standards requiring administrative, physical, and technical safeguards to protect ePHI (Office for Civil Rights, 2025). The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-66 Rev. 2 (2024) offers implementation guidance that maps HIPAA Security Rule (2024) standards and implementation specifications to practical controls for organizations of all sizes, including small practices (Marron, 2024). Recent industry statistics indicated sustained increases in hacking-related incidents and ransomware that impacted care delivery and exposed large volumes of patient records, underscoring the need for mature governance, risk management, and workforce cybersecurity practices (Alder, 2025). This proposed project focuses on Information Security Policy Development and Compliance aligned to NIST Cybersecurity Framework (CSF) 2.0 (2024) and the HIPAA Security Rule (2024), producing a set of information security policies and a compliance plan tailored to a small dental clinic setting.

RECOGNIZE AND DEFINE THE PROBLEM

Dental clinics routinely process ePHI and other sensitive data, making them attractive targets for phishing, credential compromise, ransomware, and supply-chain breaches (Alder, 2025; Wallace & Ford, 2025). The HIPAA Security Rule (2024) requires regulated entities and business associates to implement reasonable and appropriate safeguards, with flexibility to scale controls to organizational size and complexity (Office for Civil Rights, 2025). NIST CSF 2.0 (2024) provided outcome-based cybersecurity practices (e.g., Governance, Identify, Protect, Detect, Respond, Recover) that interoperated with HIPAA (2024) to reduce risk and improve resilience (Marron, 2024). Peer-reviewed work shows that human factors (e.g., phishing and unintentional errors) are primary contributors to healthcare breaches, which implies that policy, training, and access control must be foundational in small-practice settings (Yeo & Banfield, 2021; Sardi et al., 2020). Industry reporting further links ransomware and vendor-originated incidents to extended downtime and large-scale exposure of health records, demonstrating the operational and patient-care consequences when cybersecurity programs are immature (Alder, 2025).

FACTS

Platinum Dental Clinic is a small, single-site practice with 10 employees that uses a cloud electronic health record (EHR) plus commercial email/productivity tools for appointments, billing, and patient communications. However, it does not enforce unique user identifications (IDs) or multi-factor authentication (MFA), and some staff share logins for the EHR and billing, which prevents individual accountability and makes password compromise more dangerous. As a result, the clinic is not fully addressing HIPAA (2024) access control and person/entity authentication in 45 C.F.R. §§ 164.308(a)(4) (information access management), 164.312(a)(1) and 164.312(a)(2)(i) (unique user identification), 164.312(d) (person or entity authentication) (Marron, 2024; Office for Civil Rights, 2016). Cybersecurity training is informal and one-time at hire; there is no documented awareness policy, no annual refresh, and no phishing/social engineering testing. This leaves staff vulnerable to email-based attacks and misdirected disclosures, and shows the clinic is not fully meeting the cybersecurity awareness and workforce security requirements in 45 C.F.R. § 164.308(a)(5)(i) and (a)(5)(ii)(A)-(D) (security awareness and training) (Marron, 2024; Office for Civil Rights, 2016).

Encryption is inconsistent, and there is no ePHI Data Protection and Encryption Policy. This increases the chance of eavesdropping and ransomware, and means the clinic is not fully addressing confidentiality and transmission security safeguards in 45 C.F.R. §§ 164.312(a)(2)(iv) (encryption), 164.312(e)(1)-(2) (transmission security), and 164.308(b)(1) (BA data protection when transmitted) (Marron, 2024; Office for Civil Rights, 2016). System and application logs (EHR, email, etc.) exist but are not centralized, retained by policy, or reviewed regularly, so suspicious activity may go unnoticed. This is not compliant with the information system activity review in 45 C.F.R. §§ 164.308(a)(1)(ii)(D) (information system activity review), and 164.312(b) (audit controls) (Marron, 2024; Office for Civil Rights, 2016).

The clinic uses several external providers, but Business Associates (BAAs) have not been inventoried or recently reviewed, and there is no standard process for incident notification or shared responsibilities. This means it is not fully meeting 45 C.F.R. §§ 164.308(b)(1) (business associate contracts), 164.314(a)(1)-(2) (organizational requirements), and 164.308(a)(1)(ii)(D) (activity review of remote access) (Marron, 2024; Office for Civil Rights, 2016). Finally, some removable media, paper records, and networking equipment are stored in shared or unlocked areas, and there is no device/media controls or physical access policy. This shows gaps in 45 C.F.R. §§ 164.310(d)(1)-(2) (device and media controls), 164.310(d)(2)(iii) (accountability), 164.310(d)(2)(i) (disposal), 164.310(a)(1), 164.310(a)(2)(ii)-(iii) (facility access controls), 164.310(b) (workstation use), 164.310(c) (workstation security) (Marron, 2024; Office for Civil Rights, 2016).

PROJECT SCOPE AND GOALS

Develop and deliver a set of information security policies and a compliance plan mapped to HIPAA Security Rule (2024) standards and NIST CSF 2.0 (2024) outcomes for the functions Identify, Protect, and Detect (Marron, 2024; National Institute of Standards and Technology, 2024; Office for Civil Rights, 2016). The scope includes governance of policy documents, access control, workforce security, device and media protections, vendor and Business Associate oversight, data classification and retention, and centralized logging and monitoring. The scope excludes the Respond and Recover NIST CSF 2.0 (2024) pillars and detailed procedural runbooks. Incident response procedures and contingency planning will be scheduled as a future phase to complete full coverage of the HIPAA Security Rule (2024).

This project will deliver two categories of goals to remain aligned with the information security policy development and compliance plan. The managerial goals are: (MG 1) establish and approve a Cybersecurity Awareness and Training Policy that satisfies 45 C.F.R. § 164.308(a)(5)(i) and (a)(5)(ii)(A)-(D) (security awareness and training); (MG 2) establish and approve a Information System Activity Review, Audit Logging, and Monitoring Policy that satisfies 45 C.F.R. §§ 164.308(a)(1)(ii)(D) (information system activity review), and 164.312(b) (audit controls); (MG 3) establish and approve a Third-Party/Business Associate and Remote Access Management Policy that satisfies 45 C.F.R. §§ 164.308(b)(1) (business associate contracts), 164.314(a)(1)-(2) (organizational requirements), and 164.308(a)(1)(ii)(D) (activity review of remote access); and (MG 4) establish and approve a Physical Security and Facility Access Control Policy that satisfies 164.310(a)(1), 164.310(a)(2)(ii)-(iii) (facility access controls), 164.310(b) (workstation use), 164.310(c) (workstation security). The technical goals are: (TG 1) implement and document an Access Control and Authentication Policy with unique IDs and multifactor authentication to satisfy 45 C.F.R. §§ 164.308(a)(4) (information access management), 164.312(a)(1) and 164.312(a)(2)(i) (unique user identification), 164.312(d) (person or entity authentication); (TG 2) implement and document an ePHI Data Protection and Encryption Policy to support 45 C.F.R. §§ 164.312(a)(2)(iv) (encryption), 164.312(e)(1)-(2) (transmission security), and 164.308(b)(1) (BA data protection when transmitted); and (TG 3) implement and document a Device and Media Controls Policy to satisfy 45 C.F.R. §§ 164.310(d)(1)-(2) (device and media controls), 164.310(d)(2)(iii) (accountability), 164.310(d)(2)(i) (disposal). Together, these goals raise the clinic from an ad hoc posture to a repeatable and risk-informed posture within the scope of NIST CSF 2.0 (2024) functions Identify, Protect, and Detect.

RISK MANAGEMENT

Table 1 identifies the most significant cybersecurity threats to Platinum Dental Clinic based on the scenario described previously and on current healthcare and dental sector threat reporting (Alder, 2025; Sardi et al., 2020). Each threat is expressed as an event or actor that can exploit the clinic's current weaknesses. Each risk is expressed as the consequence to the clinic. Risk is linked to exactly one Action Item, which shows a direct line from problem to solution.

Table 1 - Risk Management

Rank	Cyber Threat	Cyber Risk	Likelihood	Impact	Action Item
1	Phishing or other credential based attack	Unauthorized disclosure of ePHI through a compromised or shared account due to successful phishing or other credential-based attacks	High	High	ACT-1
2	Social engineering of staff	Accidental disclosure or misdirection of ePHI by staff due to social engineering attacks (e.g., pretexting, phone or email scams)	High	High	ACT-2
3	Eavesdropping, Data Tampering and Ransomware	Interception, tampering, or malicious encryption of ePHI in transit or at rest due to eavesdropping, man-in-the-middle attacks, or ransomware	High	High	ACT-3
4	Insider Threat	Prolonged or repeated unauthorized access to ePHI due to malicious or negligent insider activity that is not detected in time	Medium	High	ACT-4
5	Supply Chain Compromise	Exposure of ePHI processed or stored by third-party vendors due to compromise of an external service used by the clinic	Medium	High	ACT-5
6	Unauthorized access through recovered or reused device or media	Exposure of ePHI stored on devices or removable media due to unauthorized access through recovered, lost, stolen, or improperly sanitized devices or media	Medium	Medium	ACT-6
7	Unauthorized physical access to clinic facilities	Exposure of ePHI or tampering with clinical systems due to unauthorized physical access to protected areas of the clinic	Low	High	ACT-7

PROPOSED SOLUTION AND ACTION PLAN

The recommended solution and action plan is a continuous program structured by the NIST CSF 2.0 (2024) functions Identify, Protect, and Detect, and validated with the McCumber Cube to maintain balanced attention to human factors, policy, and technology for confidentiality, integrity, and availability (McCumber, 2004; National Institute of Standards and Technology, 2024). All controls are mapped to the HIPAA Security Rule (2024) and to the implementation guidance in NIST SP 800-66 Revision 2 (2024) so that a small clinic can operationalize them with appropriate evidence (Marron, 2024; National Institute of Standards and Technology, 2024; Office for Civil Rights, 2016).

Table 2 - Proposed Solution

NIST CSF 2.0 (2024) Functions	NIST CSF 2.0 (2024) Category	NIST CSF 2.0 (2024) Subcategory	ACT
Identify	Asset Management	ID.AM-04: Inventories of services provided by suppliers are maintained. ID.AM-07: Inventories of data and corresponding metadata for designated data types are maintained. ID.AM-08: Systems, hardware, software, services, and data are managed throughout their life cycles.	ACT-3, ACT-5, ACT-6
Protect	Identity Management, Authentication, and Access Control	PR.AA-01: Identities and credentials are managed. PR.AA-03: Users, services, and hardware are authenticated. PR.AA-05: Access permissions are defined, enforced, and reviewed PR.AA-06: Physical access to assets is managed, monitored, and enforced.	ACT-1, ACT-5, ACT-7
	Awareness and Training	PR.AT-01: Personnel are provided with awareness and training. PR.AT-02: specialized roles trained.	ACT-2
	Data Security	PR.DS-01: Data-at-rest protected. PR.DS-02: Data-in-transit protected. PR.DS-11: Backups of data are created, protected, maintained, and tested	ACT-3, ACT-6
	Platform Security	PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk. PR.PS-04: Log records are generated and made available for continuous monitoring. PR.DS-11: Backups of data are created, protected, maintained, and tested.	ACT-4, ACT-6
Detect	Continuous Monitoring	DE.CM-01: Networks and services monitored. DE.CM-02: Physical environment monitored to find adverse events. DE.CM-03: Personnel activity and technology usage are monitored. DE.CM-06: external service-provider activities are monitored. DE.CM-09: Hardware, software, and data monitored.	ACT-4, ACT-5, ACT-6, ACT-7

Table 3 - Proposed Action Plan

No.	Action Item	Action Description	NIST CSF 2.0 (2024) Subcategories implemented	HIPAA Security Rule (2024) sections addressed	Type	Goal
ACT-1	Access Control and Authentication Policy	Develop, approve, and implement an Access Control and Authentication Policy for all ePHI systems that require unique user IDs, MFA where feasible, role-based access for clinical vs. front-desk staff, and quarterly access reviews; technical configuration must follow the policy.	PR.AA-01: Identities and credentials are managed. PR.AA-03: Users, services, and hardware are authenticated. PR.AA-05: Access permissions are defined, enforced, and reviewed.	45 C.F.R. §§ 164.308(a)(4) (information access management), 164.312(a)(1) and 164.312(a)(2)(i) (unique user identification), 164.312(d) (person or entity authentication)	Technical	TG-1
ACT-2	Cybersecurity Awareness and Training Policy	Develop, approve, and roll out a Cybersecurity Awareness and Training Policy that mandates initial and annual training, social-engineering awareness, secure workstation use, and sanctions for noncompliance.	PR.AT-01: Personnel are provided with awareness and training. PR.AT-02: specialized roles trained.	45 C.F.R. §§ 164.308(a)(5)(i) and (a)(5)(ii)(A)-(D) (security awareness and training)	Managerial	MG-1
ACT-3	Data Protection and Encryption Policy	Approve and implement an ePHI Data Protection and Encryption Policy that requires encryption for ePHI at rest (servers, workstations, laptops) and in transit (TLS-protected remote access, secure email for PHI exchanges), and inventory of ePHI data stores.	PR.DS-01: Data-at-rest protected. PR.DS-02: Data-in-transit protected. ID.AM-07: Inventories of data and corresponding metadata for designated data types are maintained.	45 C.F.R. §§ 164.312(a)(2)(iv) (encryption), 164.312(e)(1)-(2) (transmission security), and 164.308(b)(1) (BA data protection when transmitted)	Technical	TG-2
ACT-4	Information System Activity Review, Audit Logging, and Monitoring Policy	Create and enforce an Information System Activity Review, Audit Logging, and Monitoring Policy that requires audit logs on ePHI apps, daily automated log collection, weekly human review, and alerting for off-hours or suspicious access; logs must be retained per policy.	PR.PS-04: Log records are generated and made available for continuous monitoring. DE.CM-01: Networks and services monitored. DE.CM-03: Personnel activity and technology usage are monitored. DE.CM-09: Hardware, software, and data monitored	45 C.F.R. §§ 164.308(a)(1)(ii)(D) (information system activity review), and 164.312(b) (audit controls)	Managerial	MG-2
ACT-5	Third-Party/Business Associate and Remote Access Policy	Draft and enforce a Third-Party / Business Associate and Remote Access Policy that documents all supplier-provided services, requires BAAs, restricts remote sessions to approved tools, and mandates monitoring of external service-provider activity.	ID.AM-04: Inventories of services provided by suppliers are maintained. PR.AA-05: Access permissions/authorizations are defined and reviewed. DE.CM-06: external service-provider activities are monitored.	45 C.F.R. §§ 164.308(b)(1) (business associate contracts), 164.314(a)(1)-(2) (organizational requirements), and 164.308(a)(1)(ii)(D) (activity review of remote access)	Managerial	MG-3
ACT-6	Device and Media Control Policy	Approve and implement a Device and Media Controls Policy that governs receipt, movement, reuse, backup-before-move, and final disposal of any hardware or media with ePHI.	ID.AM-08: Systems, hardware, software, services, and data are managed throughout their life cycles. PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk. PR.DS-11: Data backups are created, protected, maintained, and tested. DE.CM-09: Hardware, software, and data monitored.	45 C.F.R. §§ 164.310(d)(1)-(2) (device and media controls), 164.310(d)(2)(iii) (accountability), and 164.310(d)(2)(i) (disposal)	Technical	TG-3
ACT-7	Physical Security and Facility Access Control Policy	Create and implement a Physical Security and Facility Access Control Policy to restrict access to the records room, servers, and network closet, and require visitor logs, enforce door and cabinet locking, and monitor physical areas.	PR.AA-06: Physical access to assets is managed, monitored, and enforced. DE.CM-02: Physical environment monitored to find adverse events. DE.CM-09: Hardware, software, and data monitored.	45 C.F.R. §§ 164.310(a)(1), 164.310(a)(2)(ii)-(iii) (facility access controls), 164.310(b) (workstation use), and 164.310(c) (workstation security).	Managerial	MG-4

ANTICIPATED RESULTS

This proposed project will move Platinum Dental Clinic from an ad hoc, person-dependent cybersecurity posture to a documented, policy-driven, and auditable posture that is explicitly mapped to HIPAA Security Rule (2024) requirements and to NIST CSF 2.0 (2024) outcomes. By implementing the information security policies and compliance activities defined in ACT-1 and ACT-3, the clinic will implement information security policies and a compliance plan to introduce requirements for unique user IDs, MFA where feasible, role-based access, and encryption of ePHI in transit and at rest. These policies will directly reduce the likelihood that a single compromised or shared credential exposes all patient records and will make every access attributable to a specific staff member. Policies in ACT-2 and ACT-4 will establish a repeatable cycle of cybersecurity awareness, staff accountability, and log/audit review, so that phishing, social engineering attempts, or inappropriate access are more quickly detected, reported, and corrected. Policies in ACT-5, ACT-6, and ACT-7 will formalize vendor oversight, removable media handling, and physical access control so that third-party services, reused devices, or unlocked areas no longer become "back doors" to ePHI. Operational security will improve because staff members will be required to follow information security policies for accounts, media, and facilities, and managers will have logs and documented evidence they can present to an auditor or to upper management. Communication security will improve because the policies will address email and remote-access risks, including requirements to use TLS/MFA and avoid misdirecting ePHI. Data and network security will improve because the policies will require that protected information be encrypted, monitored, and physically controlled, reducing the impact of ransomware, eavesdropping, or insider misuse.

PROPOSED COSTS

Table 4 - Proposed Costs

Equipment/service item	Performed by	ACT # addressed	Cost per item (USD)	Number of items/Hours	Total (USD)
Access Control & Authentication Policy Development (Consulting Service)	Contractor	ACT-1	$150/hr	6	$900
Cybersecurity Awareness & Training Policy Development (Consulting Service)	Contractor	ACT-2	$150/hr	4	$600
Cybersecurity Awareness Training Seats (KnowBe4)	Internal	ACT-2	$30.5/user	10	$305
Data Protection & Encryption Policy Development (Consulting Service)	Contractor	ACT-3	$150/hr	4	$600
Log Monitoring & Review Policy Development (Consulting Service)	Contractor	ACT-4	$150	4	$600
Vendor/BAA Management & Remote Access Policy Development (Consulting Service)	Contractor	ACT-5	$150/hr	3	$450
Device & Media Controls Policy Development (Consulting Service)	Contractor	ACT-6	$150/hr	3	$450
Physical Security & Facility Access Policy Development (Consulting Service)	Contractor	ACT-7	$150/hr	3	$450
Grand Total					**$4,355**

CONCLUSIONS

This project proposes to develop and deliver a HIPAA-aligned set of information security policies and a compliance plan mapped to NIST CSF 2.0 (2024) for the Identify, Protect, and Detect functions, focusing on access control, authentication, encryption, cybersecurity awareness, audit/log review, third-party/business associate agreement (BAA) oversight, device/media control, and physical/facility access. These managerial goals (MG-1 to MG-4) and technical goals (TG-1 to TG-3) directly remediate the concrete gaps the clinic has today: shared credentials, no MFA, informal training, inconsistent encryption, weak log review, incomplete BAA management, unsecured media/areas, etc. Once implemented, the clinic will be able to demonstrate that its information security policies refer to the correct HIPAA Security Rule (2024) safeguards (e.g., 45 C.F.R. § § 164.308, 164.310, 164.312) and that they are tied to CSF 2.0 (2024) subcategories. Given today's absence of formal information security policies, lack of unique IDs, and irregular monitoring, the clinic is currently operating at approximately NIST CSF 2.0 (2024) Tier 1 (Partial). After implementing the seven action items, the clinic can realistically target Tier 2 (Risk-Informed) across the scoped functions (Identify, Protect, Detect). In short, the project gives Platinum Dental Clinic a defensible, auditable, and affordable roadmap to protect ePHI and support business continuity.

REFERENCES

Alder, S. (2025, March 19). *The biggest healthcare data breaches of 2024*. The HIPAA Journal. https://www.hipaajournal.com/biggest-healthcare-data-breaches-2024/

Alder, S. (2025, October 26). *Healthcare data breach statistics*. The HIPAA Journal. https://www.hipaajournal.com/healthcare-data-breach-statistics/

Bastidas, J. A. (2020). Cybersecurity preparedness in dental healthcare organizations. *Issues in Information Systems, 21*(1), 118–124. https://iacis.org/iis/2020/1_iis_2020_118-124.pdf?utm_

Marron, J. A. (2024, February). *Implementing the health insurance portability and accountability act (HIPAA) security rule: A cybersecurity resource guide*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-66r2.pdf

McCumber, J. (2004). *Assessing and managing security risk in IT systems*. Auerbach Publications.

National Institute of Standards and Technology. (2024). *The NIST cybersecurity framework (CSF) 2.0*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Office for Civil Rights (2025). *Summary of the HIPAA security rule*. U.S. Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

Office for Civil Rights. (2016). *HIPAA security rule crosswalk to NIST cybersecurity framework*. https://www.hhs.gov/guidance/sites/default/files/hhs-guidance-documents//nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf

Sardi, A., Rizzi, A., Sorano, E., & Guerrieri, A. (2020). Cyber risk in health facilities: a systematic literature review. *Sustainability, 12*(17), 7002. https://doi.org/10.3390/su12177002

TrustRadius. (2025). *Pricing Overview for KnowBe4 Security Awareness Training*. https://www.trustradius.com/products/knowbe4/pricing?utm_source

Wallace, K., & Ford, H. (2025, June 3). *A guide to understanding cyber liability risks for dental practices*. Risk Strategies. https://www.risk-strategies.com/blog/a-guide-to-understanding-cyber-liability-risks-for-dental-practices

Yeo, L. H., & Banfield, J. (2021). Human factors in electronic health records cybersecurity breach: an exploratory analysis. *Abstract*. https://pmc.ncbi.nlm.nih.gov/articles/PMC9123525/pdf/phim0019-0001i.pdf