Conducting an Enterprise-Wide NIST Cybersecurity Framework Assessment for MediHealth Solutions Inc.

Prepared by: **Benjamin Tetteh**
Date: 5th February, 2025

This assessment evaluates the cybersecurity posture of MediHealth Solutions Inc., a mid-sized healthcare provider, using the NIST Cybersecurity Framework (CSF). It identifies vulnerabilities, assesses risk exposure, and provides a structured remediation plan to enhance security resilience. The assessment focuses on protecting patient data, ensuring HIPAA compliance, and mitigating cyber threats through policy recommendations and technical controls.

Scenario

MediHealth Solutions Inc. is a fictional mid-sized healthcare provider with 500 employees, 20 clinics across the U.S., a telemedicine platform, and a patient portal. As they handle sensitive patient data (PHI/PII), compliance with HIPAA is mandatory. Recently, the company experienced a phishing attack, compromising an employee's email account and leading to unauthorized access to patient records. In response, the Board of Directors mandated a full NIST Cybersecurity Framework (CSF) assessment to identify security gaps, prioritize risks, and improve resilience.

Assessment Scope, Goals and Risk Analysis

Scope: This assessment evaluates the cybersecurity posture of MediHealth Solutions Inc. as of February 2025. Recommendations will outline prioritized actions for a 12-month implementation period, from February 2025 to February 2026.

Goals: The goals of this task are to:

a) Assess security posture, risks, and gaps.
b) Recommend NIST-aligned controls, policies, and best practices.
c) Ensure compliance with HIPAA, NIST CSF, and NIST SP 800-53.
d) Mitigate risks related to legacy systems, human error, third-party vendors, and insufficient monitoring.

Risk Analysis

a) **Legacy Systems:** The Electronic Health Record (EHR) system runs on outdated Windows Server 2012 with no patch management. Medical IoT devices (e.g., MRI machines) use default passwords and lack network segmentation.
b) **Compliance Risks:** HIPAA audit findings flagged insufficient access controls for patient data. No formal incident response plan exists for ransomware or data breaches.
c) **Third-Party Risks:** A third-party billing vendor was recently breached, exposing MediHealth's financial data.
d) **Human Factors:** 30% of employees failed a recent phishing simulation. No cybersecurity training program exists for clinical staff.
e) **Detection Gaps:** No centralized logging or monitoring for the telemedicine platform.

NIST Cybersecurity Framework Walkthrough

The NIST Cybersecurity Framework consists of five core functions that guide cybersecurity risk management. These functions which are – Identify, Protect, Detect, Respond and Recover, form a comprehensive life cycle for addressing security challenges.

1. Identify

This function focuses on asset management, risk assessment, and governance.

Asset Inventory

Asset	Type	Description	User	Data Stored	Criticality
Electronic Health Records (EHR) System	IT System	Stores and manages patient data	IT Team	PHI, PII	High
Telemedicine Platform	IT System	Used for remote patient consultations and data exchange	Patients, staff	PHI, PII	High
Patient portal	Cloud service	Allows patients to access their health records and communicate with providers	Patients	PHI, PII	High

MRI Machine	IoT Device	Medical equipment	Staff	Patient scans	Medium
Billing & Payment processing system	Third party vendor	External financial services handling transactions	Clinic	Financial data	High
Clinical Staff	Human asset	Works at clinic	Clinic	PHI, PII	High

Risk Assessment

Asset	Vulnerability	Threat Event	Likelihood	Severity	Risk Score
EHR System	Unpatched Windows Server 2012	Data exfiltration	3	3	9
Telemedicine platform	No centralized logging or monitoring	Undetected breach	4	4	16
Patient Portal	No MFA	Data exfiltration	3	4	12
MRI Machine	Default passwords in use and lack network segmentation	Disrupt mission-critical operations	4	5	20
Billing & Payment processing system	Recently breached exposing MediHealth's financial data	Data exfiltration	4	4	16
Clinical Staff	No cybersecurity training program exists	Unauthorized access	4	5	20

Risk Matrix:

High (15–25): Immediate action required.

Medium (5–14): Address within six months.

2. Protect

The Protect function focuses on safeguards to minimize risk exposure.

Protection Measures & NIST SP 800-53 Controls, Resources, Timelines and Cost

Asset	Gap Identified	NIST Control	Recommendation / Action	Timeline	Cost
EHR System	No automated patching	SI-2, CM-3	Deploy WSUS for automated updates	6 months	$20,000
Telemedicine Platform	No monitoring	SI-4, SC-7	Deploy SIEM & IDS (Splunk, Nessus, OpenVas)	3 months	$15,000
Patient Portal	No Multi Factor Authentication (MFA)	IA-2, IA-8	Enforce MFA via Google or Microsoft Authenticator	2 weeks	$3,000
MRI Machine	Default credentials	AC-2, AC-3	Implement Role Based Access Controls (Bitwarden)	2 weeks	$2,000
	Lack of network segmentation	SC-7. AC-4, CM-7	Implement network segmentation via VLANs	1 month	$5,000
Billing System	Third-party breach	SC-12, SC-13	Encrypt data in transit & at rest	3 months	$10,000
Clinical Staff	No cybersecurity training	AT-2, AT-3	Conduct regular cybersecurity training (KnowBe4, GoPhish)	Ongoing	$13,000

MediHealth will use the following scheduled cybersecurity training calendar to improve security awareness and compliance.

Cybersecurity Training Calendar

Month	Training Topic	Target Audience	Training Method
February	Introduction to Cybersecurity & HIPAA Compliance	All Employees	Online Training & Quiz
	Phishing Awareness & Email Security		Simulation & Workshop
March	Secure Passwords & Multi-Factor Authentication	All Employees	Online Video & Quiz
April	Social Engineering & Insider Threats	IT & HR Teams	Live Webinar
May	Endpoint Security & Safe Internet Use	Remote Employees	Online Training
June	Medical IoT & Device Security	Clinical Staff	Hands-On Workshop
July	Secure Use of Telemedicine & Patient Portals	Doctors & Nurses	Interactive Session
August	Incident Response & Reporting Procedures	IT & Security Teams	Tabletop Exercise
September	Data Encryption & Secure Data Handling	Admin & Billing	Policy Review
October	National Cybersecurity Awareness Month	All Employees	Company-wide Event
November	Third-Party & Vendor Security Risks	Procurement & Legal	Risk Assessment
December	Year-End Cybersecurity Recap & Best Practices	All Employees	CEO Security Briefing
January	Phishing Awareness & Email Security Recap	All Employees	Simulation & Workshop

3. Detect

Activities in this function include continuous monitoring, threat detection technologies and security event analysis. The absence of a central logging or monitoring system means that MediHealth cannot track suspicious activities and cannot actively watch logs and system activity to detect threats in real time. A recent breach on a third-party billing vendor has also exposed MediHealth's financial data.

This has serious security implications for MediHealth and its patients. Hackers could steal patient data or hijack video calls without detection. Investigating a breach without logs could be very difficult and increase incident response time. HIPAA requires logging and monitoring for PHI access which means MediHealth could face fines, lawsuits and suffer reputational damage.

The solutions to improve the detection capabilities of MediHealth which are crucial for minimizing impact:

a) Deploy a Security Information and Event Management (SIEM) system to collect and analyze logs from all critical systems, including the telemedicine platform.
b) Deploy Intrusion Detection Systems (IDS) and Intrusions Prevention Systems (IPS) to detect unsual network traffic patterns and prevent unauthorized access.
c) Install Endpoint Detection and Response (EDR) solutions to monitor endpoint devices for signs of compromise and automate response actions.

4. Respond

To ensure a swift and coordinated response to security breaches, MediHealth must develop and implement a formal Incident Response Plan (IRP) in alignment with NIST SP 800-61 Rev. 2. The absence of an IRP can lead to delayed responses, allowing threats to spread and disrupt critical healthcare operations. This could result in regulatory penalties, legal consequences, and financial losses due to downtime and ransom payments.

To mitigate these risks, the IRP should clearly define roles, responsibilities, and escalation procedures for incident handling. Additionally, quarterly tabletop exercises should be conducted to test and refine response readiness.

Incident Response Plan

1. Roles & Responsibilities

Role	Team Member	Responsibilities
Incident Commander	CISO/IT Director	Oversee response, declare incident severity, approve critical actions.
IT Team	Network Engineers	Isolate systems, eradicate malware, restore backups.
Legal Advisor	General Counsel	Ensure HIPAA breach notifications (within 60 days), manage legal risks.
PR Lead	Communications	Draft patient/regulator notifications, manage media inquiries.
Clinical Lead	Head of Nursing	Ensure continuity of patient care during downtime.

2. Ransomware Response Procedure

Step	Action
Detection	Trigger: SIEM alerts for mass file encryption or suspicious ransomware.txt files. IT Team: Disconnect infected device from network. Clinical Lead: Switch to paper records if EHR is down.
Containment	Isolate legacy EHR server (Windows 2012) in a segmented VLAN. Block malicious IPs via firewall
Eradication	Run anti-malware scans with Malwarebytes or Microsoft Defender**.** Check No More Ransom for decryption tools. Patch vulnerabilities.
Recovery	Restore encrypted data from immutable backups (stored offline). Test EHR functionality before reconnecting to the network.
Reporting	Legal Advisor: File HIPAA breach report with HHS within 60 days. PR Lead: Notify affected patients via email/letter
Post-Incident Review	Conduct a lessons-learned meeting to analyze the incident response and identify areas for improvement.

5. Recover

This function emphasizes restoring systems and services to normal operations following a cybersecurity event. Post-incident, systems must be restored efficiently to maintain business continuity. Key activities should include:

a) Implementing regular, secure, offline backups.
b) Developing and implementing a structured business continuity plan to maintain critical healthcare operations during an incident, ensuring minimal disruption to patient care.
c) Conducting ransomware recovery drills.
d) Developing a communication plan to address public concerns and maintain trust with patients and stakeholders.

Implementation Roadmap (12-month)

Timeline	Task	KPI	Estimated Cost
1 week	Deploy MFA & RBAC	100% MFA enforcement on EHR and Patient Portal	$5,000
1 - 3 months	Upgrade EHR System	100% legacy systems patched	$20,000
1 – 3 months	Data encryption	100% data encryption across all systems	$10,000
3 - 6 months	Implement SIEM and network segmentation	90% log coverage and IoT segmentation	$20,000
Ongoing	Cybersecurity Training for Staff	Phishing failure rate <10%; HIPAA training completion >90%	$13,000

Recommendations

MediHealth Solutions Inc. must prioritize access controls and data protection to safeguard sensitive patient information. Implementing Role-Based Access Control (RBAC) will ensure employees only access data critical to their roles—for example, restricting EHR

modifications to physicians while limiting billing staff to financial systems. Pairing RBAC with Multi-Factor Authentication (MFA) for high-risk accounts and encrypting data both at rest (AES-256) and in transit (TLS 1.3) will mitigate unauthorized access. Additionally, adopting an enterprise password manager and enforcing 14-character passwords will reduce credential theft risks, while network segmentation (e.g., isolating legacy EHR systems and IoT devices on separate VLANs) will contain potential breaches.

To bolster threat detection and system resilience, MediHealth should deploy a SIEM tool to centralize logging and alert on anomalies such as mass data exports or ransomware file patterns. Complement this with an Intrusion Detection System (IDS) like Suricata to monitor IoT device traffic for malicious activity. Legacy systems require urgent attention: prioritize patching critical vulnerabilities within 24 hours and implement virtual patching for systems that cannot be immediately updated. Immutable, air-gapped backups and monthly recovery drills will ensure business continuity during ransomware attacks, while a formal incident response plan will streamline containment, HIPAA-compliant breach notifications, and recovery.

Finally, human risk mitigation is critical. Regular cybersecurity training—tailored to roles like clinical staff (phishing simulations) and IT teams (ransomware tabletop exercises)—will reduce the 30% phishing failure rate. Third-party risks can be managed through vendor cybersecurity assessments. By aligning these efforts with HIPAA and NIST CSF standards, MediHealth will not only avoid costly fines but also build patient trust through demonstrable data protection. A phased 12-month rollout, starting with RBAC/MFA and concluding with staff training, ensures manageable, measurable progress toward a robust security posture.

This version balances technical depth with readability, emphasizes outcomes, and aligns with compliance frameworks—perfect for executive summaries or portfolio case studies.

Conclusion

This assessment provides a comprehensive cybersecurity evaluation of MediHealth Solutions Inc. By implementing the recommended controls and best practices, MediHealth will enhance its security posture, ensure regulatory compliance, and protect patient data from cyber threats.

APPENDIX 1: Online Resources

1. NIST CSF Documentation: NIST Cybersecurity Framework
2. HIPAA Security Rule Checklist: HHS HIPAA Guidelines
3. Phishing training: https://www.knowbe4.com/products/security-awareness-training
4. Phishing simulator: GoPhish https://getgophish.com/
5. HIPAA Training for Healthcare Staff.
6. CISA Cybersecurity Awareness Training
7. HIPAA Breach Notification Checklist
8. CISA Ransomware Response Checklist
9. Ransomware decryptor: https://www.nomoreransom.org

APPENDIX 2: Ransomware Response Playbook

Step	Description	Responsible Team	Tick
Detection & Identification	Monitor SIEM alerts for unusual activity, file encryption patterns, or unauthorized access. Identify affected systems and endpoints.	Security Operations Center (SOC), IT Team	
Containment	Disconnect infected devices from the network. Disable compromised user accounts. Restrict further spread by isolating affected segments.	IT Team, Network Security Team	
Eradication & Investigation	Remove ransomware payloads using endpoint security solutions. Conduct forensic analysis to determine attack vector. Patch vulnerabilities.	IT Team, Digital Forensics Team	
Recovery	Restore systems from verified, uncompromised backups. Test system integrity before reconnecting to the network. Ensure data integrity.	IT Team, Business Continuity Team	
Communication & Reporting	Notify internal security teams, executives, regulators like HIPAA and affected patients if PHI/PII is compromised. Engage law enforcement if required.	Compliance Team, Legal Team, PR Team	
Lessons Learned & Prevention	Conduct post-mortem analysis. Update incident response plans and security policies. Implement additional security measures like MFA and network segmentation.	Security Team, Risk Management Team	

APPENDIX 3: Incident Handlers Checklist

Indicate “Yes”, “No” or “N/A” to answer the question and provide reasons where applicable

Yes/No	Question	Notes
	1. Preparation	
	Are all members aware of the security policies of the organization?	
	Do all members of the Computer Incident Response Team know whom to contact?	
	Do all incident responders have access to journals and access to incident response toolkits to perform the actual incident response process?	
	Have all members participated in incident response drills to practice the incident response process and to improve overall proficiency on a regularly established basis?	
	2. Identification	
	Where did the incident occur?	
	Who reported or discovered the incident?	
	How was it discovered?	
	Are there any other areas that have been compromised by the incident? If so what are they and when were they discovered?	
	What is the scope of the impact?	
	What is the business impact?	
	Have the source(s) of the incident been located? If so, where, when, and what are they?	
	3. Containment	
	a. Short-term containment	
	Can the problem be isolated?	
	1) If so, then proceed to isolate the affected systems. 2) If not, then work with system owners and/or managers to determine further action necessary to contain the problem.	
	Are all affected systems isolated from non-affected systems?	
	1) If so, then continue to the next step. 2) If not, then continue to isolate affected systems until short-term containment has been accomplished to prevent the incident from escalating any further.	
	b. System-backup	

	Have forensic copies of affected systems been created for further analysis?	
	1) Have all commands and other documentation since the incident has occurred been kept up to date so far?	
	a) If not, document all actions taken as soon as possible to ensure all evidence are retained for either prosecution and/or lessons learned.	
	2) Are the forensic copies stored in a secure location?	
	a) If so, then continue onto the next step.	
	b) If not, then place the forensic images into a secure location to prevent accidental damage and/or tampering.	
	c. Long-term containment	
	1) If the system can be taken offline, then proceed to the Eradication phase.	
	2) If the system must remain in production, proceed with long-term containment by removing all malware and other artifacts from affected systems, and harden the affected systems from further attacks until an ideal circumstance will allow the affected systems to be reimaged.	
	4. Eradication	
	If possible, can the system be reimaged and then hardened with patches and/or other countermeasures to prevent or reduce the risk of attacks?	
	i. If not, then please state why?	
	Have all malware and other artifacts left behind by the attackers been removed and the affected systems hardened against further attacks?	
	i. If not, then please explain why?	

	5. Recovery	
	Has the affected system(s) been patched and hardened against the recent attack, as well as possible future ones?	
	What day and time would be feasible to restore the affected systems back into production?	
	What tools are you going to use to test, monitor, and verify that the systems being restored to productions are not compromised by the same methods that cause the original incident?	
	How long are you planning to monitor the restored systems and what are you going to look for?	
	Are there any prior benchmarks that can be used as a baseline to compare monitoring results of the restored systems against those of the baseline?	
	6. Lessons Learned	
	Have all necessary documentation from the incident been written?	
	i. If so, then generate the incident response report for the lessons learned meeting.	
	ii. If not, then have documentation written as soon as possible before anything is forgotten and left out of the report.	
	Assuming the incident response report has been completed, does it document and answer the following questions of each phase of the incident response process: (Who? What? Where? Why? And How?)?	
	i. Can a lessons learned meeting be scheduled within two weeks after the incident has been resolved?	
	ii. If not, then please explain why and when is the next convenient time to hold it?	
	Lessons Learned Meeting	
	i. Review the incident response process of the incident that had occurred with all CIRT members.	
	ii. Did the meeting discuss any mistake or areas where the response process could have been handled better?	
	If no such conversations occurred, then please explain why?	