Strategic Security Remediation: A NIST-Based Approach for Fielder Medical Center

Elijah Olson

Western Governors University

D486 Governance, Risk, and Compliance

Introduction

Fielder Medical Center (FMC) is a healthcare facility that receives federal funding and is seeking to expand its sales of medical equipment in the local area. With this goal in mind, FMC implemented systems to manage licensing, certificates, and other relevant professional documents, information that may contain personally identifiable information (PII). These systems were implemented with both convenience and federal compliance in mind. An external security assessment was conducted out of an abundance of caution due to security concerns. The following security strategy aims to develop a practical and comprehensive approach to ensure compliance with all applicable laws, regulations, and policies.

Security Assessment Report Findings

The security assessment for FMC conducted by Pruhart Security Consulting identified multiple gaps in the security framework. According to their findings, current security controls and policies are outdated and require immediate improvements to bring them into compliance. The security and privacy plan must be realigned with the information security plan to ensure compliance and organizational needs. This includes updating the inventory/asset list to reflect systems that are still actively used by FMC, as well as completing additional risk assessments after the updates are finished. One of the most concerning findings in the Security Assessment Report (SAR) is the lack of multifactor authentication (MFA) being implemented to identify and authenticate FMC users before granting access to organizational systems.

Identified Controls

Least Privilege

Identified Risk

The current lack of least privilege implementation by FMC poses a Moderate risk to the organization's security and data (NIST, 2012). According to FIPS 199, a risk is defined as Moderate if the impact to the loss of confidentiality, integrity, or availability (CIA) would have a profound adverse effect on the organization's operation, assets, or individuals (Evans et al., 2004). This determination includes the impact of significant damage to assets and financial loss (Evans et al., 2004). With the current access available to FMC users, a non-privileged user can perform privileged functions utilizing their non-privileged account, which is in direct opposition to NIST Security and Privacy Controls as stated in AC-6 (10) (NIST, 2020). NIST controls state that privileged functions should be isolated to individuals with a need for access, so that non-privileged users are prevented from bypassing security policies, procedures, and protocols (NIST, 2020).

Remediation Decision

FMC should implement a system of least privilege within its Information Technology (IT) systems, separating system access based on duties and systems accessed. Additionally, individual access, roles, duties, and systems should be reviewed on an ongoing basis as the organizational mission and business functions change and evolve, as per NIST AC-6 (7) (NIST, 2020). Beginning to separate system access based on duties and necessary systems ensures that an individual without a need-to-know basis does not access personally identifiable information (PII) or personal health information (PHI) unnecessarily. By periodically reviewing access controls, FMC will ensure that individuals who have changed roles do not retain access to information they no longer need to know. Implementing this change will bring FMC into compliance with FedRAMP requirements related to AC-06, Least Privilege.

Plans of Action and Milestones

Identified Risk

The next area for improvement is to develop and track planned remediation actions through a regularly reviewed system, as per NIST CA-5 (NIST, 2020). NIST defines control as implementing plans of action and milestones, including updating existing plans and milestones based on findings from assessments, independent audits, and continuous monitoring of the system (NIST, 2020). FMC currently has inadequate plans of action and milestones, which present a Low risk to the organization, as these gaps may pose a limited adverse effect on FMC operations, assets, and data (NIST, 2012).

Remediation Decision

FMC's intention to create plans of action with specific milestones and regular review and update will assist in continuously meeting compliance requirements as policies, regulations, and laws continue to evolve. Creating proper Business Continuity Management (BCM) plans reduces the risk to FMC by establishing key plans that allow for minimal disruption to business operations in the event of an incident. BCM involves identifying potential threats to an organization, assessing the impact on the business if those threats were to occur, and utilizing frameworks to build an effective response to protect organizational resources, stakeholders, and reputation (DRI International, 2012). The creation of these items would bring FMC into compliance with FedRAMP requirements for CA-5 (NIST, 2020).

Continuous Monitoring

Identified Risk

The next identified insufficiency is the failure to implement Continuous Monitoring CA-7, which is defined as the implementation of a system-level strategy to continuously monitor organizational controls, metrics, and response actions designed to address controls (NIST, 2020). The failure to monitor FMC systems for compliance with organizational policy, procedures, controls, and applicable laws and regulations places a Moderate risk to the organization. Without regular monitoring of system compliance controls, FMC is at risk of non-compliance, which exposes the organization to potential adverse impacts on the system, data, finances, and/or reputation.

Remediation Decision

FMC's decision to implement a continuous monitoring system will align procedures with NIST standards, thereby increasing ongoing awareness of the current system's security and privacy position. This, in turn, will enable FMC to make informed risk management decisions (NIST, 2020). Not all procedures introduced to FMC will occur at the same frequency, as different types of controls require different review intervals (NIST, 2020). Some controls placed into production will utilize automation to support more frequent updates to necessary systems (NIST, 2020).

Risk Assessments

Identified Risk

Inadequate performance of a follow-up Risk Assessment, RA-3, once corrections have been implemented, would pose a High risk to the organization. NIST defines properly implemented risk assessments as including the integration of risk assessment results into risk management decision-making and the updating of the risk assessment when significant changes are made to the system, its operating environment, or other conditions that could potentially impact the security or privacy state of the system (NIST, 2020).

Remediation Decision

To ensure that changes made to FMC's security posture are sufficient to remediate concerns, improve FedRAMP compliance, and adequately protect PII and PHI, the organization will conduct another risk assessment upon completion of the upgrades. FMC will ensure that the follow-up assessment includes reviews of supply chain, use of all-source intelligence, dynamic threat awareness, and predictive cyber analytics (NIST, 2020). By ensuring all relevant risk assessment types are updated and conducted again, FMC takes another step toward FedRAMP compliance.

Risk Response

Identified Risk

FMC has been found to currently be lacking proper Risk Response RA-7 within its security and privacy controls. NIST defines this control as the appropriate response to findings from security and privacy assessments, monitoring, and audits based on FMC's risk tolerance (NIST, 2020). FMC is currently not adequately implementing new controls, strengthening existing controls, or providing appropriate justification for the risks it accepts (NIST, 2020). The lack of proper Risk Response poses a High risk to FMC because inadequate response to identified risks opens the organization to multiple negative repercussions that have varying impacts.

Remediation Decision

FMC must effectively implement a risk response strategy to reduce its risk posture. The introduction of proper Risk Response provides clear protocols for addressing a realized risk, including effective communication with relevant stakeholders, such as government entities. FMC has been entrusted by patients, physicians, and government officials to safeguard PHI. Additionally, to expand into the sale of medical equipment, FMC will handle additional PII. Therefore, FMC has a duty to its customers to have systems in place to provide a proper response and communication in the event of a breach (NIST, 2020).

Remediation Recommendations

There are multiple key steps that FMC needs to take to ensure that the defects found in this security assessment are remediated. The first recommendation is to address the insufficiency of the CA-5 Plans of Action and Milestones by utilizing the Risk Management Framework. The Risk Management Framework employs a risk-based approach to integrate security, privacy, and cyber supply chain risk management activities into the system's lifecycle development (NIST, 2024). This continuous system involves categorizing the system and information that is processed, stored, and in motion based on an impact analysis (NIST, 2024). The recommendation is that a Privacy Impact Assessment (PIA) be conducted to determine what data FMC utilizes and how it is used (Editor, n.d.).

Once categorization is complete, appropriate controls can be selected, and associated remediation steps can be identified for each category of data. This includes resolving issues identified in the Security Assessment Report, such as implementing the principle of least privilege and separation of duties. Least privilege involves restricting system access so that users and processes have the minimum access necessary to complete their required tasks (NIST, 2024a). Achieving this would be facilitated by implementing the principle of separation of duties, which ensures that users are not granted sufficient privileges to misuse the system independently (NIST, 2022). Part of utilizing the separation of duties involves assigning roles to determine the required access for user accounts (NIST, 2022).

Next, a risk response plan needs to be created, according to NIST, which involves creating a summary of the potential consequences of a successful exploitation of specific vulnerabilities and their associated mitigation strategies and controls (CSRC Content Editor, 2024). Ensuring that FMC has a plan in place so that each team responding to an incident is aware of their responsibilities and courses of action, including who is responsible for which activities (Six Sigma, 2024).

This response will involve conducting another security risk assessment after these corrections are made to ensure that further corrections are not necessary at this time. While the implementation of continuous monitoring must ensure FMC's security risk landscape remains within compliance, an immediate security risk assessment upon implementing these corrective measures will determine FMC's position at that time. The continuous monitoring strategy should include specific intervals for regular assessment and multiple methods to determine inadequacies in FMC's security framework.

PCI DSS Compliance

With FMC's intention to implement a point-of-sale (POS) system at its physical location, allowing customers to purchase equipment, a PCI DSS-compliant policy and system must be developed. The PCI Security Standards Council has developed the PCI Security Standards to provide compliance requirements to protect payment data throughout its lifecycle (PCI Security Standards Council, 2024). The PCI DSS Data Security Standards involve building and maintaining a secure network and systems, protecting account data, implementing a vulnerability management program, enforcing strong access control measures, regularly monitoring and testing the networks, and maintaining an information security policy (PCI SSC, 2024).

Recommendations for accomplishing this include ensuring up-to-date firewalls between external and internal networks, removing default settings on vendor equipment, a separate VLAN for all payment side equipment, implementing network monitoring systems, and implementing data encryption both in transit and at rest. The first step is to review FMC's current firewall systems to determine if they are up to date or require replacement.

Vendor defaults on network equipment allows the default credentials for network administrator accounts to be used to access the network and adjust the network equipment including security settings (CSRC Content Editor, 2024a). Immediately during initial setup all default credentials should be removed, and unique individual administrator accounts should be established for individuals requiring access to network equipment (CSRC Content Editor, 2024a). This change ensures that only authorized individuals are able to make changes to the network security settings. This will allow the other more robust recommendations discussed able to be actioned by the network administrators for FMC.

VLAN segmentation enhances network protection by making it more difficult for malicious actors to access separate areas of the internal network in the event of a breach (Cisco, 2025). Encryption of payment data at all stages in the lifecycle protects customer data by ensuring that even if it were compromised, it would be unreadable (IBM, 2021). Lastly, regular monitoring of FMC's network is crucial to determine if it continues to meet compliance requirements and to identify breaches promptly, which is paramount to a robust, PCI DSS-compliant system.

Another area of improvement to become PCI-DSS compliant is the establishment of industry recommended Anti-virus (AV) solutions. Currently, FMC does not have any AV solutions implemented on their network. It is critical to have AV solutions in place because it monitors computers and/or networks for malware and actively works to contain identified malware on the systems (Editor, n.d.-a). It is recommended to engage multiple potential vendor partners that specialize in AV solutions such as CrowdStrike, SentinelOne, and Microsoft, to determine what AV solutions they would recommend specifically for FMC's needs and associated costs. Once this information is gathered a cost-benefit analysis should be conducted and the results should be presented to enterprise leadership for a decision on which vendor to move forward with. At that point the selected AV solution should be implemented after proper testing before deploying enterprise wide.

Conclusion

Given that FMC receives federal funding, the organization must obtain and maintain compliance with FedRAMP. FMC also has a responsibility to its staff, business partners, and customers to safeguard their PII and PHI with robust security controls. The external security risk assessment conducted has identified areas for improvement. Based on this identification, recommendations have been made to improve FMC's security posture, ensuring that corrective action is implemented and further assessment is conducted to confirm remediation. These steps will help ensure that FMC is compliant with all applicable policies, regulations, and laws.

References

Cisco. (2025, May). *What Is Network Segmentation?* Cisco. https://www.cisco.com/site/us/en/learn/topics/security/what-is-network-segmentation.html

CSRC Content Editor. (2024a). *Network Administrator - Glossary | CSRC*. Nist.gov. https://csrc.nist.gov/glossary/term/network_administrator

CSRC Content Editor. (2024b). *risk response plan - Glossary | CSRC*. Nist.gov. https://csrc.nist.gov/glossary/term/risk_response_plan

DRI International. (2012). *What is Business Continuity Management | DRI International*. Drii.org. https://drii.org/what-is-business-continuity-management

Editor, C. C. (n.d.-a). *Antivirus Software - Glossary | CSRC*. Csrc.nist.gov. Retrieved August 18, 2025, from https://csrc.nist.gov/glossary/term/antivirus_software

Editor, C. C. (n.d.-b). *privacy impact assessment (PIA) - Glossary | CSRC*. Csrc.nist.gov. Retrieved August 15, 2025, from https://csrc.nist.gov/glossary/term/privacy_impact_assessment

Evans, D., Bond, P., & Bement, A. (2004). *FIPS PUB 199*. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

IBM. (2021, July 14). *What is encryption?* Ibm.com. https://www.ibm.com/think/topics/encryption

NIST. (2012). Guide for conducting risk assessments. *Guide for Conducting Risk Assessments*, *1*. https://doi.org/10.6028/nist.sp.800-30r1

NIST. (2020). Security and Privacy Controls for Information Systems and Organizations. *Security and Privacy Controlsfor Information Systems and Organizations*, *5*(5). https://doi.org/10.6028/nist.sp.800-53r5

NIST. (2022). *Separation of Duty (SOD) - Glossary | CSRC*. Csrc.nist.gov. https://csrc.nist.gov/glossary/term/separation_of_duty

NIST. (2024a). *least privilege - Glossary | CSRC*. Csrc.nist.gov. https://csrc.nist.gov/glossary/term/least_privilege

NIST. (2024b, September 24). *NIST Risk Management Framework*. NIST. https://csrc.nist.gov/projects/risk-management/about-rmf

PCI Security Standards Council. (2024). *PCI Security Standards Overview*. PCI Security Standards Council. https://www.pcisecuritystandards.org/standards/

PCI SSC. (2024). Payment Card Industry Data Security Standard Requirements and Testing Procedures Version 4.0.1. In *PCI Security Standards Council*. PCI Security Standards Council. https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf

Six Sigma. (2024, September 3). *What is a risk response plan in project management? A definitive guide*. SixSigma.us. https://www.6sigma.us/six-sigma-in-focus/risk-response-plan/