MEMORANDUM

To: **TechNova Innovations**

From: **James A. Del Ciello**

Date: **April 5, 2025**

Re: **Risk Management Framework**

Executive Summary

Project Overview: This document conveys a cyber risk management overview regarding TechNova Innovations (hereinafter referred to as TechNova). Even though this review was made with limited information, as certain assumptions were required for this assessment, the document comes with an application of an industry standard framework commonly used to address gaps and deficiencies in a firm's network cybersecurity posture.

Key Findings: The U.S. Department of Health & Human Services (HHS) provides healthcare providers cyber risk assessments (SRAs). Their methodology was deployed for this document. The HHS document shows the critical needs with recommendations that should be addressed by TechNova leadership as soon as practicable.

1. Deficiencies for basic threats and vulnerabilities.
2. Inadequacies in their security policies.
3. Absent security and workforce procedures.
4. Shortage of security and data standards.
5. Lack of security practices.
6. Shortcomings for security of business partners.
7. Non-existent or unavailable cyber contingency plans.

Please note there are other medium-to-low cybersecurity risks, some of which may also be detailed in the following pages.

Business Description: TechNova aims to transform healthcare service delivery through innovative, secure, and patient-centric technology solutions. Part of this mission is to deploy cloud-based technologies to bolster and enhance access to healthcare services for all, and by improving patient outcomes, while assuring the privacy and security of patient data worldwide. TechNova's services also operate in a highly regulated industry, where they seek to manage patient data and facilitate better telehealth services. This can be characterized by focusing on a balance between rapid technological innovation and regulatory compliance. As a result, TechNova is working within this complex landscape knowing cybersecurity threats are prevalent, all the while protecting sensitive patient information against cyber-breaches. Thankfully TechNova's infrastructure is designed for scale and resiliency that engages a growing user-base, and their systems can evolve with the latest healthcare practices and regulations. TechNova also embraces the following business objectives: 1) Expand Telehealth Services, 2) Ensure Data Confidentiality, 3) Provide Integrity, and Availability, 4) Comply with Healthcare Regulations, 5) Innovate Continuously, 6) Maintain a Robust Security Posture, and 7) Enhance Patient Engagement and Satisfaction.

Security Challenges: The critical assessments, noted above, will challenge TechNova's ability to address network cybersecurity and regulatory compliance under the Health Insurance Portability and Accountability Act of 1996 (hereinafter referred to as HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (hereinafter referred to as HITECH), as well as International Organization for Standards 127001 and the National Institute of Standards and Technology (NIST) Special Publication 800-53.

Compliance with a Risk Management Framework

Preparation: It is not clear whether TechNova has a formally defined risk tolerance, though their exposure to HIPAA-regulated patient data is clear. Critical assets include the Patient Data Management Systems (PDMS) and PDMS-T (a telehealth extension), which handle real-time patient data and communications. These systems are prioritized due to their sensitivity, regulatory scope, and operational centrality.

Categorization: Both PDMS and PDMS-T are categorized as high risks from the Federal information Processing Standards199, given their handling of electronic Personal Health Information (ePHI) and real-time patient engagement. The potential impact of compromise includes patient harm, regulatory penalties, and reputational damage. TechNova's information systems process Personal Identification Information (PII), health histories, communications, and scheduling—all classified as sensitive, pursuant to HIPAA.

Selection: Adopt NIST SP 800-53, Revision 5 High Baseline security guidelines. This includes account management (aka AC-2), cryptographic key establishment (aka SC-12), and incident handling (aka IR-4). Supplemental actions should include mandatory multifactor authentication (MFA), endpoint encryption, and staff background checks to mitigate gaps outlined in the HHS SRA.

Implementation: Security controls must be applied across endpoints and access points. Initial implementation steps include revoking or disabling shared credentials, instituting MFA for telehealth portals, and limiting access through role-based controls. TechNova must also educate staff on phishing, malware detection, and data handling protocols.

Assessment: Deploy vulnerability scans to enhance assessment methos, internal audits, and ongoing HIPAA compliance reviews. The HHS SRA already shows a 100% deficiency rating in critical areas like asset control, workforce security, and encryption. TechNova should establish a formal self-assessment cadence and commission routine external audits annually.

Authorization: Risk decisions must be signed off by an identified Security Officer (yet to be determined), and these actions should support a documented the proverbial "Plan of Action and Milestones" (POA&M). No authorization can proceed without policies, training records, and system-level access controls in place. Management must approve systems usage based on known or tolerated risks and mitigation efforts.

Monitoring: Design a real-time monitoring strategy, which includes logs with analysis, system alerts, and Security and Event Management protocols. Current logging exists but is sporadic at best and not used effectively. Scrutinize each week, along with monthly dashboards, which should highlight anomalies. Feedback loops must not only inform but also align with future training and system updates.

Conclusion

TechNova's current cybersecurity posture presents several high-risk gaps that demand immediate attention. The analysis and recommendations presented here offer a path forward, rooted upon industry Risk Management Framework standards, and reinforced by findings from the Department of Health & Human Services' SRA. Implementation of the proposed controls, noted above, will significantly reduce exposure to regulatory penalties, reputational harm, and operational disruption.

Moving forward, TechNova's leadership must prioritize establishing a formal security governance structure, beginning with clear risk ownership, the designation of a Security Officer, and the development of a living POA&M. Success in this endeavour, will not only satisfy regulatory mandates like HIPAA and HITECH, but will also bolster TechNova's mission to deliver secure, innovative, and patient-centered healthcare solutions in an increasingly constrained and cyber-hostile threat environment.