To: John Doe, CEO
From: Michael Warner
Date: June 23, 2025

Subject: A Proposal to Address Critical Compliance Gaps and Protect Your Multi-Location Pharmacy Enterprise

1. Executive Summary: The Situation and Compliance Risk

This proposal outlines several critical, unmanaged security vulnerabilities across Pharmacy's network. A significant vulnerability is that several computers have their firewall disabled or other security misconfigurations. This is observable via the Windows Security icon; which displays a red circle when such issues are present. Ignoring these known vulnerabilities means we are currently non-compliant with federal and industry regulations:

- HIPAA & HITECH Act: The failure to implement and maintain required technical safeguards and conduct ongoing risk analysis places us in a state of "Willful Neglect."
- Payment Card Industry Data Security Standard (PCI DSS): Disabled firewalls on systems that may process credit card information is a direct violation of PCI DSS requirements.
- Federal Trade Commission (FTC) Act: The FTC considers the failure to implement reasonable data security measures to be an unfair business practice and can levy significant fines.
- USE YOUR LOCAL STATE PRIVACY & BREACH LAWS (ALL STATES HAVE THEM)

2. Pharmacy's Estimated Cost for a Data Breach

A data breach resulting from these known issues would be financially devastating. For a pharmacy of our size, this would be an existential threat. The following estimates for a breach involving just REDACTED NUMBER patients illustrate that the investment in this proposed role is a small insurance premium against a catastrophic, six-figure risk.

- Total Lower Estimate: $225,000
- Total Higher Estimate: $794,200

(Detailed breakdown includes HIPAA Fines, PCI DSS Fines, Forensic Investigation, Patient Notification, Credit Monitoring, Legal Fees, and Public Relations costs).

3. Justification for an In-House Role

An IT service provider's job is primarily technical and reactive; they fix things when they break. A Security Officer's job is strategic and proactive; their purpose is to manage business risk and ensure we are meeting our legal obligations. This isn't about blaming our IT provider; their role is fundamentally different from the one I am proposing.

The fact that these security misconfigurations exist and have been known for months perfectly demonstrates this gap. From a purely technical standpoint the systems were "working," but from a compliance and risk standpoint, it's a critical failure that has exposed us to significant liability. My proposed role is not to replace IT, but to provide the internal oversight and strategy to direct IT on our security requirements, ensuring our technical setup aligns with our legal duties.

4. The Role and Investment: A Cost-Effective Solution

I am proposing two options to secure this critical business function:

- Option 1: Full-Time Information Security Officer I am proposing to fill this role for a starting salary of $50,000. This is a modest investment for a dedicated, in-house professional who will manage and mitigate a significant risk across the entire enterprise.

- Option 2 (Alternative): Hybrid Role If a full-time position is not feasible at this moment, I propose a hybrid model where I retain my current duties while formally taking on the responsibilities of the Information Security Officer. For this significant increase in professional duties, I would ask to receive a monthly stipend of $2,000 on top of my current wages. Also, a review period every 6-months in the hybrid model so we can track the progress and ensure value is being delivered before committing to a permanent change

    - Total yearly compensation would be $57,600. *(This would adjust my implementation plan to a 45-day cycle per pharmacy location after the initial 30 days at Pharmacy)*

    - *My Initial 90-Day Plan: My first 30 days will be focused on a full risk assessment of Pharmacy and remediating the most critical issues. From there, I will spend 30 days at each subsequent location to perform a risk assessment and bring it into compliance, creating a unified security posture across the enterprise.*

5. Conclusion

This proposal offers a proactive, knowledgeable, and highly cost-effective solution to protect the business you have built. I am confident that I have the skills and dedication to successfully implement this program and protect our company, our patients, and our reputation.

- *Thank you for your time and consideration*