Assignment 6.1: Instituting a Cybersecurity and Policy Legal Program

Joshua A. Wortz

University of San Diego

CSOL-599

Dr Moore

08/02/2026

Introduction

The purpose of this document is to establish a comprehensive, legally defensible cybersecurity and privacy law program for Acuity Health, designed to secure our cloud-hosted infrastructure, satisfy multi-state privacy regulations, and mitigate ongoing litigation risks. Following a critical insider threat incident that exposed sensitive electronic medical records across multiple jurisdictions, this proposal outlines a multifaceted approach to regulatory compliance, risk management, and technological resilience. By addressing the business, functional, and technical dimensions of the security program, and by providing a clear return on investment perspective for the Chief Executive Officer, this document serves as a foundational blueprint. It is designed to modernize our Microsoft Azure environment, eliminate unauthorized data exfiltration, and definitively demonstrate how rigorous cybersecurity acts as a competitive business enabler.

Part 1: The Privacy Law Program

The Business View of Acuity Health's privacy law program focuses on aligning our security objectives directly with the organization's strategic imperatives, primarily risk management, regulatory compliance, and the preservation of patient trust. Operating across state lines requires us to navigate a complex web of disparate state privacy regulations, such as the California Confidentiality of Medical Information Act (CMIA), the California Consumer Privacy Act (CCPA/CPRA), and Washington's My Health My Data Act, alongside federal mandates under the Health Insurance Portability and Accountability Act (HIPAA). From a business perspective, the recent insider threat incident underscores that data breaches directly threaten our financial stability; in fact, the average cost of a healthcare data breach has escalated to $10.93 million, making healthcare the most expensive industry for data exposure (Vats, 2025). The

business strategy mandates the creation of stringent data governance frameworks and comprehensive non-disclosure agreements to shield the organization from ongoing and future litigation. By prioritizing data integrity and implementing a Zero Trust Architecture (ZTA), the business view ensures that Acuity Health can proactively limit financial liabilities, maintain legal defensibility across state borders, and continue its rapid expansion without being derailed by class-action lawsuits or crippling regulatory penalties (Shaik, 2024).

The Functional View translates these business objectives into actionable policies, procedures, and human-centric operations. This layer dictates how our internal personnel interact with sensitive data daily. To prevent future instances of manual data scraping and identity theft, we are instituting a robust Insider Threat Program coupled with strict Identity Governance and Administration (IGA) procedures. Functionally, this means transitioning to mandatory continuous verification and role-based access control (RBAC), augmented by User and Entity Behavior Analytics (UEBA), where clinical staff only have access to the specific patient records required for their current shift (Vajragowni, 2026). Furthermore, the functional view encompasses continuous security awareness training for staff, the enforcement of Joiner-Mover-Leaver (JML) workflows to revoke access upon termination or role change immediately, and the standardization of incident response procedures. This ensures that every employee understands their legal obligations regarding patient privacy and that anomalous behaviors, such as VIP record scraping, are flagged for immediate intervention (Vajragowni, 2026).

The Technical View defines the technological architecture required to enforce our functional policies and achieve our business goals. For Acuity Health, this relies heavily on our Microsoft Azure cloud-hosted environment utilizing a Zero Trust Architecture operating on the core principle of 'never trust, always verify'. To technically thwart insider threats, we are

deploying Software-Defined Perimeters (SDP), Azure Private Link, and network micro-segmentation, which divide our cloud environment into isolated zones to prevent lateral movement and contain unauthorized access (Ul Haq, 2025). Access to our Electronic Medical Records (EMR) system is guarded by Microsoft Entra ID Conditional Access policies, enforcing risk-based multi-factor authentication (MFA) and continuous session verification. By implementing these adaptive security policies, Automated Data Loss Prevention (DLP) via Microsoft Purview, and AI-powered threat detection algorithms in Azure Sentinel, our infrastructure processes contextual signals in real time, automatically blocking unauthorized bulk data exports and enforcing our privacy policies through immutable technical controls (Vats, 2025).

Given our disproportionately small IT and security team, Acuity Health must strategically outsource specific roles to ensure continuous protection and legal defensibility. Specifically, we will outsource 24/7 Security Operations Center (SOC) monitoring and Digital Forensics and Incident Response (DFIR). Outsourcing the SOC provides us with round-the-clock threat hunting and alert triage, which is impossible to sustain internally with our current headcount. Outsourcing DFIR is critical for legal reasons; in the face of mounting litigation and HIPAA compliance investigations, we require third-party forensic experts who can maintain a strict chain of custody and provide legally admissible evidence in court. Attempting to manage complex digital forensics internally not only stretches our limited resources but also risks perceived bias or procedural errors during legal proceedings.

To further protect the organization, Acuity Health is purchasing a comprehensive cyber insurance policy. The justification for this investment is rooted directly in the financial realities of multi-state regulatory environments and our recent incident history. Cyber insurance acts as a

vital financial safety net, covering the exorbitant costs associated with specialized legal counsel, forensic investigations, mandatory patient breach notifications, and potential regulatory fines. While our transition to a Zero Trust Architecture drastically reduces our risk profile, no system is entirely impenetrable. Purchasing cyber insurance transfers residual financial risk to an insurer, which is a fiduciary necessity to ensure Acuity Health remains solvent during prolonged legal fallout. Furthermore, modern insurers often require the exact ZTA controls we are implementing, such as continuous verification and micro-segmentation, meaning our modernized security posture directly improves our insurability and enables us to secure favorable coverage terms (Ul Haq, 2025).

Part 2: CISO Leadership and ROI

To the Chief Executive Officer of Acuity Health: I recognize the significant decision you have made to reallocate operational budget funds to support our IT and cybersecurity initiatives. While security is often historically viewed as a cost center, I want to assure you that our modern infrastructure, IT systems, and cybersecurity operations are actively advancing our business and keeping us highly competitive in the urgent care market. In the healthcare sector, patient trust is our most valuable currency. By maturing our Microsoft Azure Zero Trust Architecture, we are not just locking down data; we are enabling our clinicians to work securely from any location, streamlining their access to critical EMRs without compromising patient privacy. This seamless, secure operational capability allows us to deliver faster, more reliable patient care than competitors who suffer from systemic IT outages or rely on archaic networks. Our proactive stance on multi-state privacy compliance ensures that as Acuity Health expands into new geographic markets, our technological infrastructure is already legally compliant, eliminating regulatory friction and accelerating our time-to-market.

Regarding the Return on Investment (ROI) for the newly allocated funds, we must evaluate our returns through the lens of avoided losses, operational efficiency, and hard financial metrics. The recent incident involving the manual scraping of VIP data demonstrated the catastrophic costs of inadequate insider threat controls, manifesting in HIPAA investigations, multi-state litigation, and reputational damage. The funds you have provided are directly financing our Zero Trust implementation, which empirical data shows yields an average 327% ROI within three years of deployment by dramatically reducing the likelihood of data breaches and compliance fines (Vats, 2025). Furthermore, organizations deploying these exact architectures observe a 65% drop in insider threat events and a 57% reduction in unauthorized access events within the first twelve months (Shaik, 2024; Ul Haq, 2025). By automating our access controls and compliance reporting within Azure, we are significantly reducing the manual administrative burden on our small IT team, resulting in up to a 35% reduction in annual cybersecurity operational spending (Ul Haq, 2025). In short, this investment does not just protect our bottom line from further multi-million-dollar legal liabilities; it secures our competitive advantage and establishes a scalable, legally sound foundation for our future growth.

References

Shaik, S. (2024). Implementation and challenges of zero trust architecture in network security. International Journal on Science and Technology, 15(1), 1-6.

Ul Haq, S. M. (2025). Effectiveness of zero trust architecture in securing enterprise networks. Acta Scientific Computer Sciences, 7(6), 30-40. https://doi.org/10.31080/ASCS.2025.07.0584

Vajragowni, T. (2026). Architecting large-scale identity governance frameworks for zero trust enterprises. International Journal of AI, Big Data, Computational and Management Studies, 7(2), 70-75. https://doi.org/10.63282/3050-9416.IJAIBDCMS-V7I2P112

Vats, R. (2025). Zero trust security models for cloud-based enterprise applications. International Journal of Advances in Engineering and Management, 7(4), 147-166. https://doi.org/10.35629/5252-0704147166