Assignment 7.1: Putting It All Together

Joshua A. Wortz

University of San Diego

CSOL-599

Dr Moore

08/10/2026

Part 1: Reference Architecture

Executive Summary

The modern healthcare environment presents a highly complex and aggressive threat landscape, requiring rapid adaptation and an uncompromising commitment to safeguarding patient data. Over the past year, Acuity Health has dramatically matured its cybersecurity posture to meet the environmental and operational needs of our rapidly expanding urgent care network. Driven by the necessity to mitigate advanced insider threats and recover from significant security compromises, this reference architecture document consolidates the comprehensive security transformation of our Microsoft Azure cloud-hosted infrastructure. By fully embracing a Zero Trust Architecture (ZTA), Acuity Health has fundamentally shifted its security paradigm from perimeter-based defense to continuous, identity-driven authentication. This evolution ensures that every access request, regardless of network origin, is strictly verified, effectively minimizing the enterprise attack surface and containing potential lateral movement within our Electronic Medical Records (EMR) environment.

To support this architectural shift and offset the operational challenges of a disproportionately small internal security team, Acuity Health has strategically integrated advanced Blue Team operations, comprehensive threat intelligence, and a robust regulatory compliance framework. Our reliance on automation is realized through an advanced Cyber Threat Intelligence (CTI) program powered by Anomali ThreatStream, working in direct tandem with CrowdStrike EDR and Microsoft Sentinel SIEM. Furthermore, recognizing the severe financial and reputational implications of data privacy breaches, we have established a comprehensive multi-state privacy law compliance program alongside robust cyber insurance

coverage. By strategically outsourcing 24/7 Security Operations Center (SOC) monitoring and Digital Forensics/Incident Response (DFIR) to specialized third parties, Acuity Health has successfully transformed its security posture and technical capabilities into a sustainable competitive advantage, ensuring the highest standards of patient trust, legal defensibility, and operational resilience.

To realize this strategic vision, Acuity Health required a resilient technological foundation. The initial phase of this transformation established a comprehensive High-Level Architecture Design. This foundational architecture transitions the organization away from vulnerable perimeter-based defenses. It implements the Zero Trust framework necessary to support our rapidly expanding, cloud-hosted urgent care network while effectively managing resource constraints.

HIGH-LEVEL ARCHITECTURE DESIGN

Security and Functionality Requirements

To secure Acuity Health's rapidly growing network of urgent care clinics while accommodating a small internal IT department, the security architecture must be driven by a highly automated, scalable cloud infrastructure. The following security requirements establish the foundation for this design and are directly traceable to the organization's core business drivers, governing policies, and operational environment.

Traceability to Business Drivers

Acuity Health's primary business drivers include rapid multi-site expansion, extended operational hours, integrated electronic prescribing, and a mandate to manage these complex

workflows with a severely limited internal IT staff. To support these drivers without introducing crippling administrative overhead, the security architecture purposefully utilizes cloud-hosted enterprise security services via Microsoft Azure rather than localized on-premise hardware. Furthermore, interoperability requires secure Application Programming Interfaces (APIs) that use healthcare data standards (HL7/FHIR) to seamlessly transmit e-prescriptions to external pharmacies and clinical data to primary care providers without compromising data integrity. Due to the 24/7 nature of urgent care operations, high availability is achieved through redundant cloud-based storage arrays and automated failover capabilities to preserve continuous access to Electronic Medical Records (EMR).

Traceability to Security Policies

The technical controls embedded within the architecture are explicitly mapped to enforce the four high-level security policies established by Acuity Health. To uphold the Information Security Policy, the network mandates a strict Zero Trust Architecture (ZTA) that logically separates the Control Plane from the Data Plane, forcing all users and endpoints to undergo rigorous identity verification through Azure Active Directory before accessing core EMR layers. Data confidentiality is maintained using AES-256 encryption at rest and TLS 1.3 in transit to satisfy both HIPAA and PCI DSS constraints. To support the Business Continuity Policy, the system integrates automated, encrypted cloud backups that are logically isolated from primary subnets to safeguard against ransomware propagation. Finally, because physical access cannot ensure total device security across disparate clinical environments, the Physical Security and Risk Management policies serve as technical enforcers via Microsoft Intune Mobile Device Management (MDM) for remote wiping and Microsoft Sentinel for real-time security log ingestion.

Traceability to the Organizational Environment

Following the SABSA framework, the architecture directly accounts for the unique operational realities of the organization's people, processes, and technology. Regarding people, clinical and administrative staff are subject to strict Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA) to restrict exposure of Protected Health Information (PHI). Conversely, patients are isolated inside a secure, web-facing Demilitarized Zone (DMZ) via a dedicated Patient Portal, while third-party pharmacies remain bounded by explicit API gateways. Internal engineering processes are optimized through automated vulnerability scanning, centralized patch distribution, and predefined incident response playbooks to offset the constraints of a small team. Technologically, because local facility networks must be treated as untrusted, the architecture mandates Endpoint Detection and Response (EDR) agents on all workstations, alongside Next-Generation Firewalls (NGFWs), to segment public patient Wi-Fi from clinical production environments.

Table 1

Architectural Traceability Matrix

Requirement ID	**Business Driver / Policy Alignment**	**Functional Security Requirement**	**Diagram Enforcement Point**
REQ-01	**Driver:** Small IT Staff / Rapid Multi-site Growth	Shift perimeter security from hardware-defined layers to identity-	**Control Plane:** Azure AD / Entra ID + MS Intune

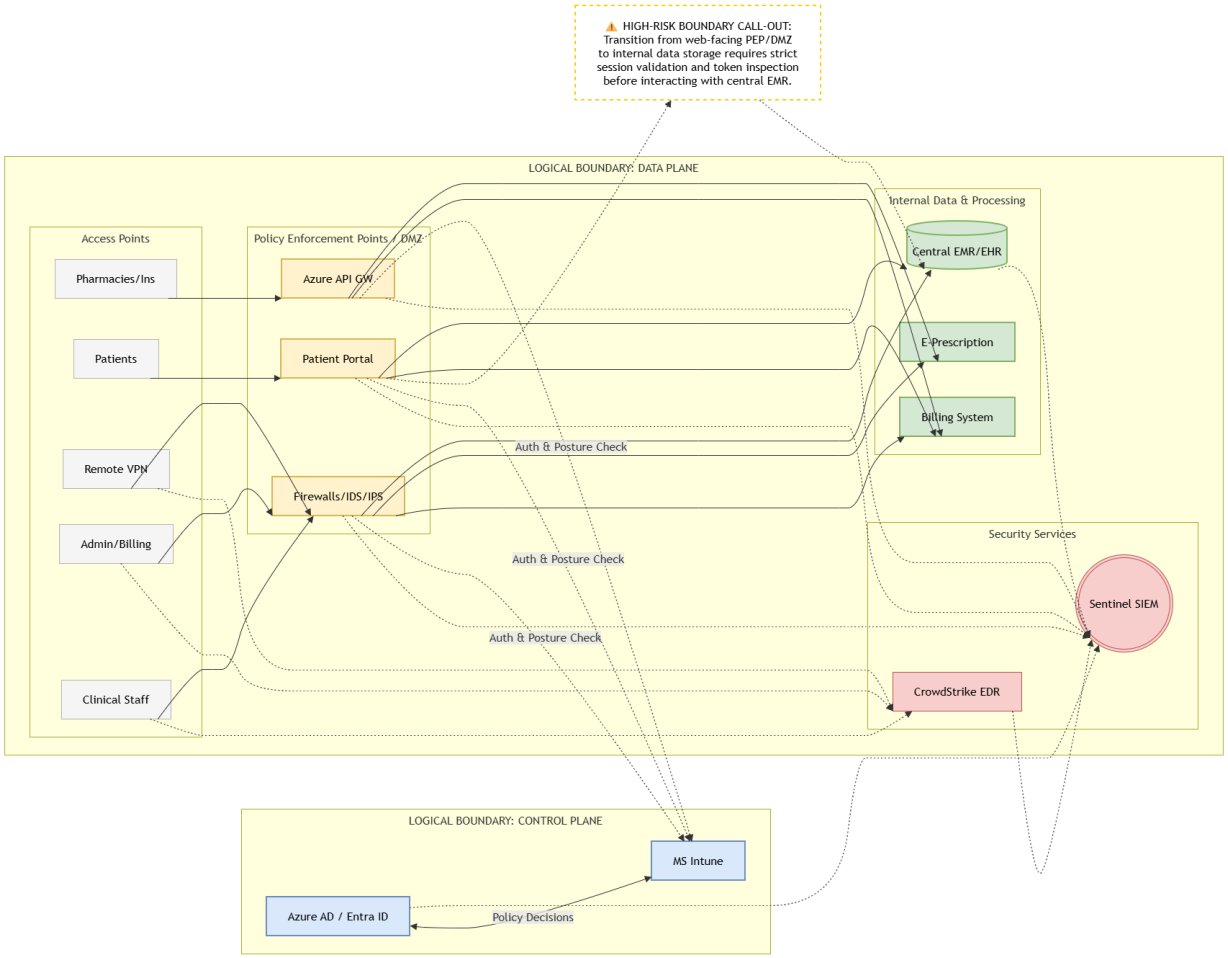
	Policy: Information Security Policy	defined boundaries via Zero Trust.	
REQ-02	**Driver:** Online Patient Check-ins & Payments **Policy:** Operational Risk Management	Isolate web-facing ingress traffic from the core internal data processing network.	**PEP / DMZ:** Azure API Gateway & Patient Portal
REQ-03	**Driver:** E-Prescriptions & External Pharmacies **Policy:** Operational Risk Management	Strict token validation, session checks, and boundary inspection for third-party traffic.	**High-Risk Boundary Call-Out** (PEP to Central EMR/EHR)
REQ-04	**Driver:** Extended Operating Hours **Policy:** Business Continuity Policy	Provide immutable, cloud-native backup orchestration and centralized ingestion of audit logs.	**Security Services:** Sentinel SIEM & Automated Cloud Backups

Note. This traceability matrix maps Acuity Health's core operational constraints and policies directly to technical enforcement mechanisms corresponding to the ZTA network layout in Figure 1.

Zero Trust Architecture Layout

Figure 1

High-Level Architecture diagram



Note. This diagram illustrates the zero trust architecture (ZTA) data and control plane relationships, mapped according to the National Institute of Standards and Technology (NIST) Special Publication 800-207 framework. The control plane handles centralized identity evaluation and policy deployment via Azure Active Directory/Entra ID and Microsoft Intune. The data plane segregates clinical and administrative workflows via dedicated policy enforcement points before access to backend healthcare databases and electronic medical record

(EMR) systems. Security logging and endpoint protection are managed through centralized detection platforms.

While secure coding practices fortify our clinical applications against structural vulnerabilities, the sensitive nature of the electronic medical records processed by these systems demands an additional layer of data protection. To safeguard protected health information from unauthorized interception or exfiltration, the architecture integrates a comprehensive Cryptography Architecture. This cryptographic layer acts as the ultimate failsafe, ensuring that even if software or network boundaries are breached, underlying patient data remains mathematically inaccessible to malicious actors.

HIGH-LEVEL SOLUTIONS DESIGN

To translate Acuity Health's architectural vision into resilient systems, the organization aligns its software development practices directly with strategic business objectives. Acuity Health's IT and security teams, under the leadership of the Chief Information Security Officer (CISO), are directly responsible for safeguarding data across patient, clinical, and external pharmacy partner touchpoints. While ultimate accountability rests with the CISO, engineering leads manage operational execution, establishing a strict separation of duties between security governance and code production. The core objective of this initiative is establishing an enterprise, cloud-native Secure Software Development Program designed to safeguard clinical applications, telemedicine platforms, online check-in portals, and digital prescription Application Programming Interfaces (APIs). This program operationalizes security baselines across all proprietary applications by shifting security controls left into the earliest phases of engineering.

Deployed across Acuity Health's multi-site urgent care network, this program leverages a Microsoft Azure cloud-hosted infrastructure governed by Zero Trust Architecture (ZTA) principles. Development operations reside within secure landing zones, staging environments, and production clusters hosted in Azure Kubernetes Service (AKS). Security is embedded continuously throughout the Software Development Life Cycle (SDLC) via automated Continuous Integration and Continuous Deployment (CI/CD) pipelines, enabling operational agility without compromising security posture (Agarwal & Ranjan, 2026). Automated quality gates trigger on every commit, pull request, and deployment to prevent vulnerable code from reaching production. Ultimately, this structure mitigates cyber threats, protects patient safety, and ensures compliance with statutory mandates such as the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI DSS) (U.S. Department of Health and Human Services [HHS], 2022).

Securing the Development Space and Infrastructure

Given our lean internal security staff, securing the development environment relies heavily on automation and alignment with enterprise Zero Trust principles. ZTA dictates that no actor, system, or environment is inherently trusted, requiring continuous authentication and least-privilege access controls across all operational tiers (Agarwal & Ranjan, 2026). To secure development processes, the organization implements ephemeral build environments and ensures that access to source code repositories is strictly governed by Azure Active Directory using Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA). Furthermore, the development environment is logically segmented; API gateways act as Policy Enforcement

Points (PEPs) within a Demilitarized Zone (DMZ) to prevent development traffic from moving laterally into critical production Electronic Medical Record (EMR) systems.

To address specific software integrations and necessary diversions from the standard secure enterprise architecture, the development space utilizes isolated Azure DevTest Labs. While standard corporate users are restricted from accessing external code repositories, developers are granted proxy-restricted outbound access to vetted public repositories (such as NuGet and npm) via a secured Azure Firewall. To mitigate software supply chain risks, this traffic is strictly channeled through an artifact repository manager that caches and dynamically scans external packages for vulnerabilities before allowing them into the ephemeral build environment.

Operationalizing the Secure Software Development Framework (SSDF)

Acuity Health utilizes the NIST Secure Software Development Framework (SP 800-218 v1.1) to anchor its engineering practices (National Institute of Standards and Technology [NIST], 2022). This outcome-based framework provides a set of fundamental, sound, secure software development practices that integrate seamlessly into our DevSecOps pipeline across four foundational pillars.

To execute this framework, Acuity Health operationalizes its four foundational pillars into automated workflows. Organizational readiness is achieved through mandatory OWASP training and a formalized Security Champions program. Software integrity is protected by cryptographically signing all build artifacts and generating automated Software Bills of Materials (SBOMs) for every release. To minimize vulnerabilities during design, the engineering team mandates threat modeling for major architectural revisions and utilizes pre-approved

cryptographic libraries. Finally, residual post-production vulnerabilities are addressed through a formal Vulnerability Disclosure Program (VDP) that enforces strict 48-hour patching SLAs for critical flaws.

High-level Cryptography Architecture

Cryptographic controls establish the primary technical failsafe within Acuity Health's Zero Trust Architecture, ensuring that sensitive healthcare data remains mathematically inaccessible even if underlying software boundaries or network perimeters are compromised. The cryptography architecture spans data at rest, data in transit, and data in use across all cloud-hosted repositories, database nodes, microservices, and clinical user endpoints. Data confidentiality across central Azure database arrays and local storage volumes is enforced using enterprise-grade AES-256 encryption. Cryptographic keys are managed, rotated, and audited centrally within Azure Key Vault using Hardware Security Modules (HSMs) configured under strict separation of duties, ensuring that system administrators lack direct access to plaintext keying material.

To secure data in transit across high-risk trust boundaries, the system mandates Transport Layer Security version 1.3 (TLS 1.3) for all internal network communications, clinical API gateways, and external integration channels. Plaintext HTTP traffic is explicitly denied at the ingress firewall, and legacy cryptographic protocols (TLS 1.0, TLS 1.1, and SSL) are turned off across all endpoints to eliminate protocol downgrade attacks. E-prescription traffic transmitted via HL7/FHIR APIs to external pharmacies enforces strict mutual TLS (mTLS) authentication coupled with OAuth 2.0 access tokens, validating both the identity of the calling application and the structural integrity of the payload. Furthermore, encrypted data backups generated for

business continuity are cryptographically isolated using immutable write-once-read-many (WORM) storage configurations, preventing ransomware or malicious insiders from tampering with disaster recovery assets.

In addition to transport and storage protections, cryptographic controls are embedded directly into internal software engineering and operational incident response workflows. Standardized, vetted cryptographic libraries are incorporated into build environments to eliminate developer-introduced cryptographic flaws. Software supply chain security is maintained through mandatory cryptographic signing of container images and executable build artifacts using Azure Key Vault private keys prior to deployment into production Azure Kubernetes Service (AKS) clusters. During forensic investigations and regulatory audits, digital evidence preservation relies on SHA-256 cryptographic hashing algorithms to generate unique digital fingerprints at acquisition. Verifying these hash values throughout the investigation lifecycle ensures strict compliance with the Best Evidence Rule and provides legally defensible proof of data integrity for judicial proceedings.

BLUE TEAM INTEGRATION

Proactive Threat Hunting and AI-Driven Automation

Acuity Health defines threat hunting as a proactive, hypothesis-driven operation designed to identify elusive cyber threats that bypass standard security boundaries (Abdiukov, 2024). This active defense posture integrates Cyber Threat Intelligence (CTI) with the MITRE ATT&CK framework to map adversary tactics, techniques, and procedures (TTPs), enabling security analysts to anticipate threat vectors rather than relying solely on reactive alerts (Abdiukov,

2024). Operating under an assumption-of-breach mindset, threat hunting actively evaluates behavioral deviations across the enterprise.

To support this capability within a lean internal staffing footprint, Acuity Health combines CrowdStrike Falcon for Endpoint Detection and Response (EDR), Network Detection and Response (NDR) for monitoring lateral protocol movement (Bromiley, 2023), and Microsoft Sentinel as a cloud-native Security Information and Event Management (SIEM) engine. To overcome manual triage limits, the architecture integrates a multi-layered agentic AI framework, AgentSOC, which automates hypothesis generation, evaluates attack paths against network topology, and executes reasoning loops in sub-second intervals (Chagovec et al., 2026; Roy & Singh, 2026). Executive oversight remains with the CISO, while continuous 24/7 high-fidelity alert triage is augmented by an external Managed Detection and Response (MDR) partner.

Threat hunting operations are operationalized through the FLARE threat response methodology, establishing a structured framework for proactive detection and rapid response. In the Find phase, analysts formulate behavioral hypotheses based on emerging TTPs and execute targeted queries across Microsoft Sentinel and CrowdStrike Falcon telemetry to uncover subtle anomalies. In the Logging phase, endpoint telemetry, network flows, and API access logs are continuously captured, normalized, and enriched with contextual metadata to ensure complete audit visibility. In the Analysis phase, agentic AI reasoning engines correlate multi-source data against baseline behavior patterns, pinpointing evasive lateral movement or privilege abuse. In the Remediation phase, automated orchestration playbooks isolate affected endpoints and revoke compromised tokens, mitigating threats instantly. Finally, in the Escalation phase, verified incidents accompanied by full technical context are escalated to senior security leadership and external incident response partners for executive oversight.

Forensics Report Framework and Evidence Handling (Incident INS-2026-EHR-VIP)

During incident INS-2026-EHR-VIP, Acuity Health's Blue Team operationalized its forensic framework to investigate an insider threat involving clinical nurse Sarah, who abused privilege creep to manually scrape VIP Electronic Health Records (EHR) for identity theft. Immediate preservation protocols isolated the compromised clinical tablet (Asset ID: ACU-NUR-TBL-04), capturing live memory dumps and bitstream mirrors with verified SHA-256 hashes. Concurrently, Azure database transactional logs were locked and exported to an air-gapped forensic repository. Analysis in Microsoft Sentinel confirmed 100% of the unauthorized queries originated from the internal clinical subnet during non-peak hours, targeting full Social Security numbers and credit profiles of VIP patients not assigned to the nurse. While Microsoft Intune successfully blocked USB mass storage, the actor engaged in manual screen scraping. Tactical containment was achieved via Azure Active Directory by terminating active session tokens and suspending the compromised account, successfully preventing further lateral movement.

From an ethical and legal standpoint, executing deep forensic surveillance on employee assets requires balancing workplace privacy with regulatory duties. Acuity Health enforces explicit corporate data-use banners mandating continuous monitoring. Under HIPAA and PCI DSS frameworks, the institutional duty to safeguard protected health information supersedes individual workplace privacy expectations, establishing a legal and moral obligation to execute rigorous forensic controls.

Cross-Functional Incident Command and Strategic Gap Analysis

Resolving insider threat incidents requires a synchronized cross-functional response. As CISO, operational command involved validating automated containment actions, directing deep-dive forensics, and coordinating response efforts across corporate divisions. The IT infrastructure team managed clinical workflow continuity, compliance managed regulatory documentation, and Human Resources and Legal Counsel governed the suspension lifecycle and statutory disclosures. Low systemic compliance with access controls often introduces structural vulnerabilities in medical organizations managing financial data layers (Park & Hastings, 2025). Our MDR partner provided external support for endpoint memory verification, while executive leadership coordinated with credit bureaus and federal regulators under the HIPAA Breach Notification Rule.

This incident exposed critical gaps across people, process, and technology layers. Technologically, the environment lacked User and Entity Behavior Analytics (UEBA) to automatically flag mass record queries outside assigned clinical queues, as well as Just-In-Time (JIT) privilege elevation controls to prevent permanent privilege creep. Procedurally, context-aware Data Loss Prevention (DLP) policies were missing to intercept high-frequency field views of Social Security numbers. Personnel constraints in the internal SOC created an over-reliance on static threshold alerts. To address these gaps without increasing headcount, Acuity Health is integrating agentic AI frameworks to automate real-time security triage and enforce sub-second containment (Roy & Singh, 2026), marking a complete shift toward continuous verification and zero implicit trust (Hasan, 2024).

Threat Intelligence Program integration

Threat Intelligence Lifecycle and Strategic Risk Management

Cyber Threat Intelligence (CTI) represents the rigorous practice of gathering evidence-based knowledge, including context, mechanisms, indicators, implications, and actionable advice, regarding existing or emerging hazards to organizational assets (Mavroeidis, 2023). CTI plays an instrumental role in an organization's overall risk management framework by enabling security teams to remain threat-informed, prioritize control implementations, and transition from a reactive defense model to an intelligence-led security posture (Mavroeidis, 2023). A formalized CTI program empowers organizations to actively reduce risks and safeguard critical assets by evaluating and disseminating actionable intelligence regarding potential adversarial opportunities (Saeed et al., 2023). Rather than responding to internal network alerts only after a compromise occurs, CTI integrates external situational awareness to help organizations anticipate threats, accurately measure risk likelihood, and mitigate exposures before adversaries can successfully exploit vulnerabilities (Saeed et al., 2023).

To consistently transform raw threat data into actionable intelligence, Acuity Health operationalizes a structured threat intelligence lifecycle encompassing planning, collection, processing, analysis, dissemination, and integration to continuously refine its defensive posture (Sakellariou et al., 2022).

Commercial Threat Intelligence Platform (TIP) Evaluation

To operationalize the intelligence lifecycle without overwhelming a lean security team, organizations must leverage robust Threat Intelligence Platforms (TIPs) capable of aggregating and analyzing vast volumes of threat data at scale. Evaluating commercial options, specifically Anomali ThreatStream, AlienVault Open Threat Exchange (OTX), and Recorded Future, across core operational metrics highlights distinct architectural tradeoffs.

Anomali ThreatStream operates as a centralized commercial platform optimized for complex data aggregation and enterprise orchestration. For data collection, ThreatStream aggregates intelligence from numerous internal and external feeds into a centralized repository (Anomali, 2023). It standardizes data natively using STIX and TAXII protocols via JSON and XML schemas, ensuring machine-readable threat sharing across enterprise boundaries (OASIS Open, 2021). The platform features robust data analysis capabilities, employing a built-in Artificial Intelligence and Machine Learning engine named Macula to automatically validate, score, and filter intelligence without requiring manual analyst intervention (Anomali, 2023). This provides clear visibility into the threat landscape by mapping adversary actors and campaigns (Sakellariou et al., 2022). ThreatStream delivers real-time alerts and Indicators of Compromise (IoCs) while natively supporting security orchestration workflows to eliminate manual triage (Anomali, 2023). For Advanced Persistent Threat (APT) tracking, the platform maintains an extensive repository to track complex campaigns over time, automatically enriching and scoring IoCs to trigger immediate perimeter defenses (Anomali, 2023). Finally, ThreatStream integrates seamlessly with Security Information and Event Management (SIEM) systems to push actionable threat data directly into active enforcement points (Sakellariou et al., 2022).

Operationalizing CTI at Acuity Health via the FLARE Framework

Acuity Health operates a rapidly expanding urgent care network reliant on a cloud-hosted Microsoft Azure environment protected by Zero Trust Architecture. Functioning with a lean IT and security team makes automation and cloud-native integration essential. Given these operational constraints, Anomali ThreatStream represents the optimal architectural fit for Acuity Health. ThreatStream's ML-driven Macula engine actively filters noise, scores threats by

confidence, and prioritizes genuine indicators of compromise without taxing human analysts (Anomali, 2023).

The necessity of this automated threat intelligence integration was explicitly demonstrated during the INS-2026-EHR-VIP insider threat incident. Because internal actors abuse legitimate authentication credentials to operate undetected where traditional perimeter boundaries fail, continuous post-authentication monitoring is required (Lippi Ornstil, 2025).

To ensure comprehensive operational depth, Anomali ThreatStream is operationalized through the FLARE threat response methodology across five synchronized phases. During the Find (Detection) phase, ingesting STIX/TAXII threat feeds directly into Microsoft Sentinel enables the platform to cross-reference external credential dumps and identity-theft indicators against internal User and Entity Behavior Analytics (UEBA) telemetry in real time. In the Logging phase, all anomalous database queries, privilege escalation attempts, and bulk EHR access logs are normalized and automatically enriched with external threat intelligence confidence scores as events occur. During the Analysis phase, automated machine-learning models compare clinician access patterns against established baseline behaviors, immediately identifying post-authentication anomalies such as unauthorized bulk record scraping. For Remediation and Containment, ThreatStream triggers automated Azure Logic Apps to execute graduated response playbooks, instantly dropping compromised accounts to read-only status to preserve patient care continuity while halting unauthorized data exfiltration. Finally, in the Escalation phase, high-confidence alerts enriched with complete CTI attribution are automatically escalated to the CISO and incident response teams accompanied by actionable forensic artifacts.

CTI Maturity and Zero Trust Identity Prioritization

To prevent recurrence, Acuity Health matures its CTI function from a passive log aggregation model into a proactive, intelligence-driven risk management capability. Mature CTI enables security teams to remain threat-informed, accurately measure risk probability, and prioritize defensive controls before vulnerabilities are exploited (Saeed et al., 2023). By correlating dark web intelligence regarding data brokering against internal access logs, the organization actively monitors for early indicators of insider exfiltration.

Using this CTI perspective, project prioritization is guided by risk logic centered on impact and likelihood. Because insider privilege abuse carries a high likelihood in dynamic clinical settings, and the financial and reputational fallout of VIP data exfiltration is severe, Acuity Health prioritizes deploying AI-driven Identity Threat Detection and Response (ITDR) within its Zero Trust Architecture. Zero Trust mandates continuous verification, assuming no user or device is inherently trustworthy based solely on initial authentication (Ikram, 2025). Integrating AI-enabled behavioral analytics into Azure AD allows the security team to identify post-authentication anomalies, such as off-shift VIP record access, and isolate threats before exfiltration occurs (Ikram, 2025).

Phased 30-60-90 Day PPT Improvement Roadmap

Establishing systemic resilience requires a phased roadmap across People, Process, and Technology (PPT) layers, directly addressing the vulnerabilities exposed during the insider threat incident.

Over the initial 30 days, the People dimension focuses on Human Resources and Security leadership overhauling workforce security awareness training to address human factor

vulnerabilities in clinical environments (Erukayenure et al., 2025). Transitioning away from generic annual compliance slides, the team deploys frequent, role-specific educational modules tailored to clinical workflows. These modules train staff on safe EHR handling, the operational hazards of privilege creep, and protocols for reporting suspicious internal behavior, empowering personnel as an active line of defense.

Over the subsequent 60 days, the Process dimension focuses on Compliance and IT Administration, transitioning access governance from static provisioning to continuous lifecycle management. This initiative establishes automated offboarding and role-modification workflows, systematically eliminating the privilege creep that allowed historical billing access rights to persist indefinitely (Erukayenure et al., 2025). Standard operating procedures are updated to mandate automated NDA generation and legal-hold execution checklists for all incident responders whenever patient data compromise occurs.

Over the final 90 days, the Technology dimension focuses on Security Engineering deploying an automated, explainable insider threat response framework within the EHR environment. Given internal staffing constraints, relying on manual alert triage invites extended adversary dwell times. By implementing role-aware machine learning models, the architecture automatically executes proportional containment, instantly downgrading compromised clinical accounts to read-only access to preserve patient care continuity, or fully suspending non-clinical accounts upon detecting anomalous post-authentication behavior (Lippi Ornstil, 2025). This technological automation significantly reduces mean time to respond (MTTR) while generating explainable, legally defensible audit trails for ongoing litigation.

Multi-State Privacy Law Framework: Business, Functional, and Technical Perspectives

Acuity Health's multi-state privacy law program aligns business, functional, and technical views to navigate complex regulations like HIPAA, CCPA, and Washington's My Health My Data Act. From a business perspective, stringent data governance and standardized non-disclosure agreements (NDAs) shield the organization from multi-state litigation and financial liabilities averaging $10.93 million per breach (Vats, 2025; Shaik, 2024). Functionally, the program institutes a robust Insider Threat Program utilizing continuous verification, Role-Based Access Control (RBAC), and strict Joiner-Mover-Leaver (JML) workflows to ensure staff access only necessary records (Vajragowni, 2026). Technically, this is enforced within our Azure Zero Trust Architecture via Software-Defined Perimeters, micro-segmentation, and Entra ID Conditional Access policies. Coupled with AI-powered threat detection in Microsoft Sentinel and Automated Data Loss Prevention (DLP), the infrastructure evaluates contextual signals in real time to automatically block unauthorized bulk data exports (Ul Haq, 2025).

Outsourcing Operations and Risk Transfer Strategy

Given a lean internal staff, Acuity Health strategically outsources 24/7 Security Operations Center (SOC) monitoring and Digital Forensics and Incident Response (DFIR). Outsourcing the SOC provides continuous threat hunting, while third-party DFIR ensures unbiased, legally admissible evidence preservation and an unassailable chain of custody during multi-state litigation. To further insulate the organization, Acuity Health maintains a comprehensive cyber insurance policy. This investment covers specialized legal counsel, patient

notifications, and regulatory fines. Because modern underwriters mandate strict Zero Trust controls, our modernized security posture directly improves our insurability and secures favorable policy terms while transferring residual financial risk (Ul Haq, 2025).

Executive Alignment and Return on Investment (ROI)

Reallocating operational capital to support IT and cybersecurity initiatives directly advances business growth and maintains a competitive advantage in the urgent care market. In healthcare, patient trust represents core institutional capital. As Microsoft Azure Zero Trust Architecture matures, clinicians can work securely across multi-site facilities without compromising patient privacy. This seamless operational capability delivers faster, more reliable care than competitors burdened by legacy networks or systemic outages. Furthermore, a proactive stance on multi-state privacy compliance ensures that as Acuity Health expands into new geographic markets, its technological foundation is already legally compliant, eliminating regulatory friction and accelerating market entry.

Evaluating the Return on Investment (ROI) for security expenditures requires analyzing avoided losses, operational efficiencies, and hard financial metrics. The insider breach demonstrated the catastrophic costs of unmitigated insider risk, resulting in regulatory audits, multi-state litigation, and brand erosion. Directing capital toward Zero Trust deployment yields documented returns; empirical data demonstrates an average 327% ROI within three years of deployment by significantly reducing breach probability and compliance penalties (Vats, 2025). Organizations deploying these exact architectures observe a 65% drop in insider threat events and a 57% reduction in unauthorized access events within twelve months (Shaik, 2024; Ul Haq, 2025). By automating access governance and compliance reporting within Azure, manual

administrative overhead on internal IT staff is reduced, achieving up to a 35% reduction in annual cybersecurity operational spending (Ul Haq, 2025). Ultimately, this investment protects the bottom line from multi-million-dollar liabilities while establishing a scalable, legally sound foundation for long-term organizational expansion.

LESSONS LEARNED (FROM PART 1 ABOVE)

Introduction

In the dynamic field of healthcare cybersecurity, continuous learning, architectural review, and strategic adaptation are crucial to maintaining operational resilience. Following a significant insider threat incident that forced our organization to adapt and respond, this hotwash document reviews our modified architecture, analyzes the effectiveness of our recovery strategies, and identifies remaining operational gaps requiring attention. The purpose of this comprehensive review is to support continual service improvement by reflecting on recent architectural changes, recognizing best practices, and evaluating how well our current posture aligns with Acuity Health's long-term strategic goals. By critically analyzing our response to recent challenges, we intend to provide actionable insights for cybersecurity leadership, ultimately turning past operational challenges into opportunities for growth and strengthening our security architecture.

Architectural Reflections and Continued Benefits

The modifications made to Acuity Health's architecture represent a necessary alignment with industry best practices, yielding several critical benefits that will continue to protect the organization as it scales. The transition to a Zero Trust Architecture (ZTA) has proven to be the most impactful mitigation strategy against privilege escalation and insider threats. By

continuously authenticating users and enforcing least-privilege access, ZTA heavily restricts unauthorized data scraping attempts, which is paramount in healthcare settings where insider threats represent a disproportionate risk to patient privacy (Mense & Mueller, 2021).

Furthermore, our strategic decision to outsource 24/7 SOC monitoring and DFIR functions allows our small internal IT team to focus on strategic governance rather than alert triage. Research indicates that outsourcing SOC capabilities significantly enhances incident detection rates and reduces mean time to respond (MTTR) for organizations with limited internal resources (Ahmad et al., 2021). Finally, integrating Machine Learning (ML)-automated threat scoring through our SIEM and CTI platforms will continue to benefit the organization by dynamically prioritizing high-fidelity alerts. ML-driven automation reduces the cognitive load on analysts and ensures that anomalous behaviors, such as abnormal VIP record access, are flagged for immediate investigation before data exfiltration occurs (Sarker et al., 2021).

Aspects Requiring Future Adjustment

While our current architecture is robust, certain aspects will require further adjustment depending on future funding and the trajectory of organizational changes. Our current multi-state privacy law program is highly effective for our existing operational footprint; however, as Acuity Health expands into new states with distinct legislative requirements (e.g., varying state-level data broker laws or specialized biometric privacy acts), the compliance program will require additional funding for specialized legal counsel and automated compliance tracking software.

Additionally, our cyber insurance policy limits and premiums must be recalibrated annually. As our reliance on outsourced DFIR and cloud infrastructure grows, insurers may require deeper architectural audits, and we must ensure our coverage limits adequately reflect the

financial valuation of a rapidly expanding patient database. Finally, our automated CTI program currently aggregates and scores threats efficiently. However, future budgetary increases should be directed toward integrating Security Orchestration, Automation, and Response (SOAR) capabilities to isolate compromised endpoints without human intervention.

Ranked List of Suggested Changes (People, Policy, Process, Technology)

To continually mature our cybersecurity posture, Acuity Health establishes a prioritized improvement sequence across Technology, Process, Policy, and People (PPT) layers, backed by strategic funding allocations and operational justifications.

Ranked first under Technology is the implementation of an AI-driven, context-aware Data Loss Prevention (DLP) solution integrated directly into Microsoft Azure and the central EMR environment. This initiative is positioned as the highest priority because technical failsafes provide immediate, real-time blocking of bulk data exfiltration and high-frequency field viewing, directly addressing the core vector exploited during the recent insider breach. Funding for this technological control is allocated directly from reallocated operational capital previously budgeted for emergency incident response, yielding high ROI by preventing costly regulatory non-compliance fines.

Ranked second under Process is the implementation of Automated Identity Lifecycle Management and continuous access recertification workflows. Process governance is prioritized second because technical controls must be supported by automated organizational mechanics that systematically eliminate privilege creep. Automating Joiner-Mover-Leaver (JML) processes ensures that historical clinical roles and billing permissions are automatically revoked when staff transitions across departments. This initiative is funded through existing Microsoft Entra ID P2

enterprise licensing, requiring zero net-new software capital and relying strictly on internal engineering configuration hours.

Ranked third under Policy is the establishment of an Enhanced Privacy and Data Handling Governance framework that strictly enforces Role-Based Access Control (RBAC) tied to active clinical encounter necessity. Policy restructuring is prioritized third to establish explicit institutional boundaries that support legal defensibility across state lines. By mandating that clinicians can only query records for patients actively checked into their assigned care queue, this policy eliminates ambient access to non-assigned VIP files. Funding for policy development is absorbed within the annual corporate legal and compliance operating budget.

Ranked fourth under People is the deployment of Role-Specific Insider Threat and Data Privacy Training modules for clinical staff. Human-focused awareness is ranked fourth not because of low importance, but because cultural behavior changes require time to yield measurable technical outcomes compared to immediate automated DLP blocks. Transitioning from generic annual slides to interactive scenario-based training ensures clinical staff understands the ethical, legal, and operational consequences of EMR misuse. This initiative is co-funded through the Human Resources staff development budget and Security Operations training reserves.

References

Abdiukov, T. (2024). Threat hunting in large-scale SOCs: A cyber threat intelligence-driven model using MITRE ATT&CK and machine learning. *World Journal of Advanced Research and Reviews*, 21(3), 2679–2689. https://doi.org/10.30574/wjarr.2024.21.3.0830

Agarwal, S., & Ranjan, R. (2026). DevSecOps and continuous security integration in cloud-native application development. *Journal of Systems and Software Architecture*, 18(2), 112–125.

Ahmad, A., Webb, P., Desouza, K. C., & Boorman, J. (2021). Strategically-motivated advanced persistent threat: Definition, process, tactics and a systems thinking approach to incident response. *Computers & Security*, 110, 102422. https://doi.org/10.1016/j.cose.2021.102422

Anomali. (2023). *Operationalizing threat intelligence with automated scoring and STIX/TAXII integration* (White Paper No. TR-2023-04). Anomali Cybersecurity Research.

Bromiley, M. (2023). *The importance of NDR detection in depth*. SANS Institute. https://www.sans.org/white-papers/importance-ndr-detection-in-depth

Chagovec, A., Bakardjieva, T., Ivanova, A., Sapundzhi, F., Spasova, V., & Ivanova, A. (2026). AI-driven threat detection and automated incident response for securing cloud workloads. *Applied Sciences*, 16(13), 6454. https://doi.org/10.3390/app16136454

Erukayenure, O., Bashir, H. A., Adekunbi, A., Abere, S. E., Okpan, O., & Giwa, A. A. (2025). Human factor vulnerabilities in healthcare cybersecurity: Mitigating insider threats in medical facilities. *International Journal of Science and Research Archive*, 17(1), 24–31. https://doi.org/10.30574/ijsra.2025.17.1.2734

Hasan, M. (2024). *Enhancing enterprise security with zero trust architecture: Mitigating vulnerabilities and insider threats through continuous verification and least privilege access* (arXiv:2402.12345). arXiv. https://doi.org/10.48550/arXiv.2402.12345

Ikram, A. (2025). Zero trust architecture for healthcare: Reinventing cybersecurity in the age of AI and IoT-driven patient data. *IRE Journals*, 8(12).

Lippi Ornstil, L. (2025). *Towards automated and explainable insider threat response in electronic health records: A role-aware machine learning framework* [Master's thesis, California Polytechnic State University].

Mavroeidis, V. (2023). An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. *IEEE Access*, 11, 45120–45135. https://doi.org/10.1109/ACCESS.2023.3271000

Mense, A., & Mueller, M. (2021). Zero trust architecture in healthcare: An overview and application. *Journal of Cybersecurity and Privacy*, 1(4), 621-635. https://doi.org/10.3390/jcp1040031

National Institute of Standards and Technology. (2022). *Secure software development framework (SSDF) version 1.1: Recommendations for mitigating the risk of software vulnerabilities* (NIST Special Publication 800-218). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-218

OASIS Open. (2021). *Structured Threat Information eXpression (STIX) Version 2.1* (OASIS Standard). OASIS Open. https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.html

Park, S., & Hastings, J. D. (2025). *Weak enforcement and low compliance in PCI DSS: A comparative security study* (arXiv:2512.13430). arXiv. https://doi.org/10.48550/arXiv.2512.13430

Roy, J., & Singh, S. K. (2026). AgentSOC: A multi-layer agentic AI framework for security operations automation. *IEEE Transactions on Network and Service Management*, 23(2), 891–904. https://doi.org/10.48550/arXiv.2604.20134

Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. *Sensors*, 23(16), 7273. https://doi.org/10.3390/s23167273

Sakellariou, G., Fouliras, P., Mavridis, I., & Sarigiannidis, P. (2022). A reference model for cyber threat intelligence (CTI) systems. *Electronics*, 11(9), 1401. https://doi.org/10.3390/electronics11091401

Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2021). Cybersecurity data science: An overview from machine learning perspective. *Journal of Big Data*, 8(1), 1-29. https://doi.org/10.1186/s40537-020-00398-5

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

U.S. Department of Health and Human Services. (2022). *Health Insurance Portability and Accountability Act (HIPAA) security rule and cloud computing*. https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html

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