Assignment 4.1: Implementing Key Security Systems with Active Defense Part 2

Joshua A. Wortz

University of San Diego

CSOL-599

Dr Moore

07/20/2026

Part 1. Computer Forensics Report Framework and Evidence Collection

Incident Reference: INS-2026-EHR-VIP

Organization: Acuity Health

EXECUTIVE SUMMARY

Acuity Health recently experienced a severe internal data security incident within its cloud-hosted urgent care network involving the unauthorized access, systematic extraction, and subsequent external exploitation of highly sensitive patient records. The active threat stemmed from an insider incident involving a long-term, trusted clinical nurse, Sarah, who leveraged persistent privilege creep to view electronic health records well beyond her assigned clinical scope and operational necessity. Over an extended duration, the internal actor abused administrative billing-review permissions to repeatedly query and exfiltrate personal data from patient profiles explicitly designated with a high-profile VIP classification tag. The incident was detected retrospectively when the corporate compliance team executed a targeted electronic health record audit and identified severe behavioral anomalies that directly correlated with external breach inquiries submitted by victimized clients to the Information Office regarding fraudulent loans and credit cards established in their names. In response, the Chief Information Security Officer immediately suspended access to the compromised credentials, isolated the target endpoint assets, mobilized the internal incident response framework, and engaged an external Managed Detection and Response vendor to conduct a comprehensive technical and legal forensic examination.

Evidence and Custodians

Evidence

Forensic evidence collection was initiated immediately following the incident declaration on July 17, 2026, targeting the clinical assets and cloud nodes associated with the compromised user session. The primary physical evidence container consists of a bit-stream forensic duplicate of the mobile clinical workstation tablet assigned to the urgent care nursing floor, designated as Asset ID ACU-NUR-TBL-04. To preserve data integrity and satisfy the legal parameters of the Best Evidence Rule, a cryptographic digital fingerprint was generated at the exact moment of acquisition, resulting in a verified SHA-256 hash value of e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855. The secondary evidence container consists of a cloud snapshot export of the centralized Azure-hosted Electronic Health Record database transaction logs spanning the exact period of the anomaly, which was cryptographically secured with a generated SHA-256 hash value of 8f434346648f6b96df89da901c5467ae45a43b9044ca495991b7852b855f4321.

Custodians

The sole corporate custodian of the physical hardware, operating system configurations, and cloud infrastructure repositories under inspection is Acuity Health Corporate Headquarters, located at 100 Corporate Parkway, Oceanside, California, 92056. The lead security engineer managed operational custody of the physical clinical tablet during the collection phase under the direct supervision of the Chief Information Security Officer. The logical cloud environments and database clusters remain under the administrative custody of the internal cloud infrastructure

team, governed by strict enterprise role-based access control policies to prevent unauthorized manipulation or chain-of-custody contamination throughout the lifecycle of the forensic review.

3 Methodology

3.1 Preservation

The preservation of digital evidence within Acuity Health's cloud-hosted infrastructure relied entirely on cryptographically validated active defense playbooks designed to safeguard volatile metadata and maintain strict legal compliance. Upon verification of the anomalous activity, the security engineering team immediately performed logical isolation of the physical clinical tablet from the primary enterprise wireless network plane. The device was kept powered on to prevent the destruction of volatile random-access memory, active cryptographic keys, and open application session tokens. Using enterprise-grade forensic software suites and a hardware write-blocker, analysts captured a comprehensive live memory dump, followed by a full bitstream mirror of the local storage blocks. Simultaneously, write locks were applied to the Azure cloud database nodes, converting the live transactional logs into read-only containers and exporting them directly to an air-gapped forensic repository to ensure that no post-incident data alteration or log deletion could occur.

3.2 Analysis

The analytical methodology employed a multi-layered correlation technique to translate raw cloud telemetry and endpoint artifacts into a defensible narrative of insider-threat behavior. Investigators ingested the aggregated logs within the cloud-native Security Information and Event Management platform, Microsoft Sentinel, to map the complete query timeline executed

under Sarah's user account. Forensic analysts cross-referenced the automated application-layer database timestamps with the internal physical nursing shift logs and clinical check-in queues. Endpoint analysis was conducted using CrowdStrike Falcon behavioral telemetry to determine whether automated scraping scripts, external cloud storage connections, or local hardware mass storage devices were initiated on the clinical tablet. This comprehensive technical review focused on analyzing the structural context of the access, verifying the specific data elements viewed, and demonstrating intent by highlighting the complete lack of operational clinical justification for the queries.

4 Findings

4.1 Location

Forensic evaluation of the network infrastructure logs confirmed that 100% of the unauthorized electronic health record queries originated from the internal clinical subnet of the main urgent care facility. The media access control addresses and local Internet Protocol records extracted from the Azure API Gateway verified that the network traffic was tied exclusively to the wireless interface of the specific nursing floor workstation tablet, Asset ID ACU-NUR-TBL-04. There was no evidence of external network ingress or geographic spoofing, proving that the exploit was executed entirely within the physically trusted domain of the clinical facility.

4.2 EHR VIP Database Transaction Analysis

The application-layer database analysis revealed a systematic, intentional pattern of data scraping targeting high-value patient files. Sarah's authenticated user identity successfully queried the records of every single patient designated with the VIP classification tag across the enterprise database. The time-series data demonstrated that these records were accessed

repeatedly, often in dense chronological clusters during non-peak operational intervals. The logs confirmed that the data fields viewed included full Social Security numbers, complete residential addresses, private health insurance identifiers, and secondary financial credit profiles. Crucially, cross-referencing clinical tracking records proved that Sarah had never been assigned to assist, treat, or intake any of the victimized clients, thereby completely invalidating the legitimacy of the administrative billing review privileges she was using.

4.3 Identity Theft Correlation and External Indicators

The technical findings directly explain the external fraud indicators that the enterprise's Information Office received. The specific patient accounts accessed during Sarah's unauthorized database sessions perfectly match the identities of the clients who reported that fraudulent lines of credit and external credit cards had been opened in their names. Endpoint analysis verified that, while Sarah did not use unauthorized USB mass storage devices or automated scripting tools, which were successfully blocked by enterprise Microsoft Intune policies, she engaged in manual screen scraping, transcribing the displayed personal identifiers directly from the clinical tablet screen during periods of financial distress driven by mounting personal debt.

5 Ethical Implications

5.1 Privacy, Informed Consent, and Regulatory Protections

Executing an intensive forensic investigation into the behavior of a long-term, trusted employee introduces complex ethical considerations regarding internal privacy boundaries, corporate surveillance, and institutional trust. Acuity Health balances these factors by maintaining strict adherence to explicit corporate data use policies, ensuring that all endpoint

monitoring and device audits are governed by pre-established consent banners that mandate regular monitoring to optimize security and compliance. From a regulatory perspective, the ethical duty to safeguard patient confidentiality under HIPAA and PCI DSS frameworks supersedes any individual workplace privacy expectations. The organization bears an absolute moral and legal responsibility to ensure that sensitive protected health information is never exploited to harm clients, necessitating the implementation of rigorous forensic controls to maintain institutional integrity, protect victimized patients, and support lawful external regulatory investigations.

6 Conclusion and Incident Response Framework

The forensic investigation into incident INS-2026-EHR-VIP has successfully established a validated, cryptographically sound reconstruction of the internal data compromise at Acuity Health. Through rigorous SHA-256 hashing and bitstream duplicate analysis, the security engineering team has demonstrated that the clinical nurse, Sarah, abused legacy administrative permissions to scrape sensitive patient records systematically. The digital evidence collected from the physical tablet and the Azure database logs remains pristine and legally defensible, providing definitive proof of unauthorized access to full Social Security numbers and credit profiles. This technical assessment concludes the formal forensics pipeline, establishing the empirical foundation required for subsequent corporate governance actions, employee disciplinary proceedings, and mandatory federal regulatory reporting cycles.

Part 2. Incident Response Report

Incident Definition and Chronological Reconstruction

Acuity Health's security operations team has established a comprehensive understanding of the active insider threat incident affecting the centralized cloud-hosted electronic health records environment. The incident involved an authorized user privilege abuse by Sarah, a long-term and highly trusted clinical nurse at the urgent care facility. Over an extended period, Sarah experienced severe financial distress driven by mounting personal debts, establishing the behavioral catalyst for the insider exploit. Exploiting permanent privilege creep, which occurred when her user account was granted elevated administrative rights to assist with historical billing review inquiries, Sarah bypassed standard clinical boundary restrictions.

This elevated access permitted the retrieval of full Social Security numbers, residential addresses, health insurance information, and financial credit profiles. Sarah systematically targeted and queried the database records of every single patient carrying a high-profile VIP classification tag. Because she engaged in manual screen scraping and physical transcription directly from her assigned mobile clinical tablet rather than using automated data exfiltration scripts, the activity did not trigger initial volume-based perimeter alerts. The exfiltrated personal identifiers were subsequently leveraged to establish fraudulent lines of credit and external consumer credit cards, impacting victimized clients who initiated data breach inquiries with the Information Office. The operational breach perimeter was formally declared following a retrospective data audit by the compliance team, confirming a profound departure from core Zero Trust principles, in which internal trust must never be implicitly granted based on institutional longevity or clinical standing (Hasan, 2024).

Security Tooling Efficacy in Investigation and Remediation

The technical investigation, containment, and subsequent remediation protocols utilized Acuity Health's core enterprise security architecture, revealing distinct variable operational efficiencies across our cloud infrastructure. Microsoft Sentinel served as the cloud-native Security Information and Event Management platform, functioning as the centralized collection engine for retrospective log aggregation and timeline reconstruction. While Sentinel enabled the security team to correlate database transactions, historical evaluations underscore that traditional SIEM detection models face significant visibility limitations when analyzing advanced internal threats that use authorized credentials, as they lack out-of-the-box behavioral modeling context (Putri, 2025).

For endpoint verification, the team deployed CrowdStrike Falcon analytics to audit the volatile memory state and application processes running on the compromised nursing workstation tablet. Falcon verified that the local operating system remained uncompromised, confirming that no malicious secondary software or automated extraction kits had been introduced into the local clinical subnet. Microsoft Intune functioned as the device compliance administrator, verifying that baseline BitLocker encryption remained fully active during the physical seizure of the hardware asset. Active tactical remediation was driven by Azure Active Directory, which served as the critical point of policy enforcement. The engineering team utilized Azure Active Directory to instantly terminate active session tokens, rotate root database access credentials, and enforce global account suspension for Sarah's identity plane, successfully invalidating cached authentication parameters before the internal threat actor could pivot into broader clinical API architectures.

Critical Forensic Evidence Catalysts

The discovery and correlation of multiple distinct indicators of technical and behavioral evidence drove the directional momentum of this investigation. The primary application-layer evidence consisted of EHR transactional access logs that revealed a massive, statistically anomalous density of user queries targeting the specialized VIP patient database segment. Time-series analysis performed by the security engineering team demonstrated that these intensive database reads occurred in tightly packed chronological clusters that did not align with Sarah's assigned nursing shifts, clinic operating schedules, or open patient check-in queues.

Furthermore, clinical tracking records confirmed that Sarah had never provided direct clinical assistance, triage, or intake workflows for any of the accessed VIP clients, establishing definitive proof of unauthorized intent. This internal digital evidence was matched against the external fraud reports compiled by the Information Office, confirming that the specific patient records scraped from the clinical tablet perfectly mirrored the identities of the clients experiencing active credit exploitation. The lack of local system modification or USB mass storage connectivity confirmed that manual screen transcription was the exclusive exfiltration mechanism.

Cross-Functional Incident Response Team and External Support

Resolving this trusted insider incident required a tightly synchronized, multi-tiered response framework that spanned distinct corporate divisions and specialized external vendors to manage operational dependencies and regulatory requirements. As Chief Information Security Officer, I retained direct operational command over the technical response, steering the security engineering group through log analysis and validating containment playbooks. The internal information technology infrastructure team managed clinical workflow continuity by executing

the logical lockout of the compromised tablet workstation while maintaining alternative clinical systems to prevent operational disruption across the urgent care centers. The corporate compliance team retained ownership over initial audit discovery, validation, and regulatory documentation.

Because the threat was executed by an active, long-term employee, Human Resources and Corporate Legal Counsel were integrated immediately into the incident command structure to govern the suspension lifecycle, preserve statutory employee disclosure rights, and limit organizational corporate liability. Navigating the severe data exposure boundaries highlighted that low systemic compliance with strict access controls frequently introduces structural vulnerabilities in medical organizations that manage complex financial data processing layers (Park & Hastings, 2025). To supplement the lean internal staff, Acuity Health mobilized its third-party Managed Detection and Response vendor, dedicating specialized forensic analysts to validate endpoint memory dumps and cross-verify network telemetry. Externally, executive leadership coordinated with credit monitoring bureaus to protect affected clients and prepared formal notifications to federal regulatory authorities under the HIPAA Breach Notification Rule.

Strategic Gap Analysis: People, Process, and Technology

This active insider incident exposes severe, systemic gaps across Acuity Health's people, processes, and technology layers that must be aggressively remediated to establish a defensible active defense posture. From a technological perspective, the primary architectural vulnerability is the complete reliance on reactive, periodic compliance audits rather than real-time, behavior-based alerting pipelines within our cloud-native SIEM engine. Securing high-volume cloud workloads processing sensitive data requires integrating AI-driven threat detection models that continuously analyze heterogeneous telemetry to automatically intercept internal privilege abuse

in real time (Chagovec et al., 2026). The environment was entirely missing User and Entity Behavior Analytics, which can automatically flag a nursing credential executing mass queries outside assigned clinical queues. Furthermore, the identity footprint lacked just-in-time privilege-elevation controls, causing permanent privilege creep by leaving administrative billing access active indefinitely rather than restricting it to time-bound, monitored windows.

Procedurally, the enterprise lacked context-aware data-loss prevention policies engineered to intercept or block high-frequency views of data fields containing full Social Security numbers and credit card numbers within the EHR interface. From a personnel perspective, the lean staffing model of the internal security operations center created an absolute dependency on static, automated threshold alerts that were blind to authorized insider context, leaving a critical operational gap in human oversight. To alleviate these severe constraints without expanding headcount, the organization requires a multi-layer agentic AI framework, such as AgentSOC, to automate real-time security operations triage, enabling the system to validate internal attack paths and execute automated containment logic within sub-second thresholds (Roy & Singh, 2026). Ultimately, these findings dictate an immediate shift away from implicit internal trust toward a model enforced by continuous verification, automated behavioral analytics, and multi-tier authorization gates for all high-sensitivity classification tags.

References

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

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

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

Putri, D. G. (2025). *Analysis of the effectiveness of security information and event management (SIEM) detection against advanced threats.* Greenation International Journal of Engineering Science (GIJES), 3(3), 159–165.

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