A black and blue logo

Description automatically generated

The Heart Hospital

SOC 2 Audit Report (Type 1)

Information Systems  
June 1, 2024

Legal Disclaimer  
*This document is intended solely for academic research purposes and does not constitute an official SOC 2 Type 1 audit report. The findings, conclusions, and recommendations presented herein are based on hypothetical scenarios and academic analysis and should not be interpreted as a formal audit conducted by a certified professional. The Heart Hospital, Baylor Scott & White Health, and any referenced entities are used as part of an academic exercise and not as part of an actual assessment. For official audit and compliance services, please consult a certified public accountant or a qualified audit firm.*

Table of Contents

1. **Introduction**
2. **Scope of Audit**
3. **Management’s Assertion**
4. **Description of the System**
   * EpicCare Link
   * Vulcan PACS
   * TVU Networks
   * Azure and Oracle SQL Data Storage
5. **Control Environment**
6. **Risk Assessment**
   * Risk Assessment Process
   * Risk Mitigation Strategies
7. **Control Activities**
   * Security Controls
   * Confidentiality Controls
8. **Information and Communication**
9. **Monitoring of Controls**
10. **Tests of Operating Effectiveness and Results**

* Access Control Tests
* Multi-Factor Authentication (MFA) Tests
* Encryption Tests
* Monitoring and Logging Tests
* Incident Response Tests
* Confidentiality Agreement Compliance Tests

1. **Identified Risks and Findings**
2. **Recommendations**
3. **Vendor Security Assessment Integration**
4. **Training and Awareness Initiatives**
5. **Conclusion**
6. **References**

**1. Introduction**

This SOC 2 Type 1 audit report evaluates the design and implementation of controls within The Heart Hospital, focusing on the trust service criteria of Security and Confidentiality. The audit assesses the controls related to systems including EpicCare Link, Vulcan PACS, TVU Networks, and Azure/Oracle SQL Data Storage as of June 1, 2024. This report provides a comprehensive analysis of the hospital’s control environment, risk management processes, control activities, and the effectiveness of these controls in maintaining the security and confidentiality of sensitive patient data.

**2. Scope of Audit**

The audit encompasses the following systems, integral to the operation of The Heart Hospital:

* **EpicCare Link**: A web-based platform enabling healthcare providers to access patient medical records in real-time.
* **Vulcan PACS**: A medical imaging system for storing, retrieving, and managing diagnostic images.
* **TVU Networks**: A secure video communication platform used for real-time consultations and diagnostics.
* **Azure Cloud Services**: The platform hosting various hospital applications and providing scalable data storage solutions.
* **Oracle SQL Database**: A database managing patient information and critical hospital data, crucial for maintaining the integrity and availability of healthcare operations.

**3. Management’s Assertion**

The management of The Heart Hospital asserts that:

* The description of the system within The Heart Hospital, including all relevant components such as EpicCare Link, Vulcan PACS, TVU Networks, and Azure/Oracle SQL Data Storage, is fairly presented and accurately reflects the current state of our IT environment.
* The controls related to Security and Confidentiality have been suitably designed and implemented to provide reasonable assurance that the hospital’s service commitments and system requirements will be achieved based on the trust service criteria of Security and Confidentiality.
* Specific controls, including those related to access management, encryption, vendor security assessments, and staff training, are designed to mitigate identified risks such as ransomware attacks, insider threats, and data breaches.
* We have implemented a comprehensive risk management process, including continuous monitoring and periodic evaluations, to ensure that the controls remain effective and responsive to emerging threats.
* Management is committed to the ongoing improvement of these controls and will take corrective actions to address any gaps or weaknesses identified during this audit or through our internal risk assessments.

**4. Description of the System**

**EpicCare Link**  
EpicCare Link is a critical web-based application that integrates with the main Epic EHR system, allowing healthcare providers to access patient medical records securely in real-time. This system employs role-based access control (RBAC), multi-factor authentication (MFA), and robust encryption to ensure data security and confidentiality during patient care processes.

**Vulcan PACS**  
Vulcan PACS is an advanced medical imaging system used for the storage, retrieval, and management of diagnostic images such as X-rays, CT scans, and MRIs. This system is fully integrated with EpicCare Link, ensuring seamless access to imaging results for healthcare providers. Vulcan PACS employs strong encryption for data at rest and in transit, along with comprehensive audit logging for all access and modification actions, ensuring compliance with security policies.

**TVU Networks**  
TVU Networks provides secure, real-time video communication capabilities, essential for remote consultations and time-sensitive diagnostic procedures within the Hospital. This system is particularly valuable for enabling specialists to provide diagnostic and treatment recommendations rapidly, even in complex cases. The platform includes encrypted communication channels, ensuring that all transmitted data remains confidential and secure.

**Azure and Oracle SQL Data Storage**  
The hospital’s IT infrastructure leverages Azure cloud services for hosting critical applications and providing scalable data storage solutions. Patient information is securely stored in Oracle SQL databases, with Azure offering the necessary infrastructure to support high availability and disaster recovery. Both Azure and Oracle SQL employ industry-standard encryption protocols and are configured to meet the stringent security requirements of healthcare operations.

**5. Control Environment**

The control environment at The Heart Hospital is meticulously designed to ensure the secure and confidential operation of its systems. This environment is characterized by a robust organizational structure, a commitment to ethical standards, and the clear assignment of authority and responsibility. The hospital’s IT and information security teams are pivotal in maintaining this environment, with a strong emphasis on compliance with regulatory requirements and the protection of patient data.

**Organizational Structure**  
The hospital’s IT department is structured to provide comprehensive support for the secure operation of all critical systems. The Chief Information Officer (CIO) oversees IT operations, including security and compliance. The Information Security Officer (ISO) is responsible for implementing and maintaining security controls, while department heads ensure that their teams adhere to established policies and procedures.

**Ethical Standards and Policies**  
The Heart Hospital enforces a robust Code of Conduct, which outlines the ethical standards expected of all employees. This code is reinforced through regular training and awareness programs, ensuring that all staff members understand their responsibilities regarding the security and confidentiality of patient data.

**6. Risk Assessment**

**Risk Assessment Process**  
The Heart Hospital conducts an annual risk assessment to identify and manage potential risks that could impact the security and confidentiality of its systems. This process involves collaboration between the IT department, senior management, and external consultants to ensure a comprehensive evaluation of potential threats. Key risks identified during the assessment include ransomware attacks, insider threats, and data breaches, each of which is evaluated based on its potential impact on patient care and the hospital’s reputation.

**Risk Mitigation Strategies**  
To address the identified risks, The Heart Hospital has implemented a series of mitigation strategies, including:

* **Ransomware Response Plan**: A comprehensive plan designed to detect, respond to, and recover from ransomware attacks. This plan includes regular backups, disaster recovery testing, and staff training to ensure preparedness.
* **Insider Threat Monitoring**: The deployment of advanced tools and processes to detect and respond to potential insider threats, including unusual access patterns and unauthorized data access.
* **Encryption and Access Controls**: The use of robust encryption methods and strict access controls to protect sensitive patient data from unauthorized access and ensure compliance with industry standards.

**7. Control Activities**

**Security Controls**  
The security controls at The Heart Hospital are designed to ensure the protection of patient data and the secure operation of critical systems. These controls include a combination of automated and manual processes, supported by comprehensive policies and procedures.

* **Access Controls**: RBAC is implemented across all critical systems, ensuring that users have access only to the information necessary for their job functions. MFA is required for accessing all critical systems, providing an additional layer of security against unauthorized access.
* **Encryption**: Data at rest is encrypted using AES-256, while data in transit is protected using TLS 1.2 or higher. These encryption methods ensure that patient data remains secure, even in the event of a security breach.
* **Monitoring and Logging**: Crowdstrike Endpoint Protection is deployed across all endpoints, providing real-time threat detection and response capabilities. Detailed audit logs are maintained for all access and modification actions, supporting incident investigation and ensuring compliance with security policies.

**Confidentiality Controls**  
Confidentiality controls are designed to protect patient data from unauthorized access and ensure compliance with privacy regulations.

* **Data Classification**: All patient data is classified according to its sensitivity, with the highest level of protection applied to personally identifiable information (PII) and medical records.
* **Access Control**: Access to patient data is restricted to authorized personnel who require it to perform their job duties. Access requests are reviewed and approved by the Information Security Officer.
* **Confidentiality Agreements**: All employees are required to sign confidentiality agreements upon hiring, acknowledging their responsibility to protect patient data and comply with hospital policies.

**8. Information and Communication**

The Heart Hospital’s information and communication systems are designed to support the secure and efficient operation of its healthcare services. These systems include secure communication channels, policies for information sharing, and procedures for reporting incidents.

**Secure Communication Channels**  
TVU Networks provides encrypted video communication channels for real-time consultations and diagnostics. The system is integrated with the hospital’s secure network, ensuring that all communications are protected from unauthorized access.

**Information Sharing**  
Internal communication regarding security policies, procedures, and incidents is facilitated through the hospital’s intranet and regular staff meetings. The Information Security Officer is responsible for ensuring that relevant information is disseminated promptly to all staff members.

**Incident Reporting**  
Incident response procedures are outlined in the hospital’s Incident Management Policy. All employees are trained to report security incidents, including potential data breaches, phishing attempts, and suspicious activity, to the Information Security Officer immediately.

**9. Monitoring of Controls**

**Continuous Monitoring**  
The Heart Hospital employs continuous monitoring to ensure that security and confidentiality controls are operating effectively.

* **Crowdstrike Endpoint Protection**: This tool provides real-time monitoring of all endpoints, with alerts for any suspicious activity or potential threats. The system’s performance is reviewed regularly to ensure it meets the hospital’s security requirements.
* **Audit Log Reviews**: Audit logs from critical systems, including EpicCare Link, Vulcan PACS, and Oracle SQL databases, are reviewed monthly by the Information Security Officer to detect any unauthorized access or modifications.

**Periodic Evaluations**

* **Annual Risk Assessment**: The hospital’s risk assessment process includes an annual review of the effectiveness of security and confidentiality controls. This review involves testing controls, evaluating their effectiveness, and making adjustments as needed.
* **External Audits**: The Heart Hospital engages external auditors annually to review its security and confidentiality controls and ensure compliance with regulatory requirements.

**10. Tests of Operating Effectiveness and Results**

In the SOC 2 Type 1 audit, extensive tests were conducted to evaluate the effectiveness of controls related to the security and confidentiality of The Heart Hospital’s systems. These tests were designed according to industry standards, including the Common Criteria for Information Technology Security Evaluation (CC) and NIST Special Publications.

**Access Control Tests**

* **Tested Control**: Role-based access control (RBAC) for EpicCare Link, Vulcan PACS, and Oracle SQL databases.
* **Procedure**: A review of user access permissions was conducted to ensure alignment with the principles of least privilege and job responsibilities. A sample of user accounts was selected, and their access permissions were compared against job roles and responsibilities. The process of granting, modifying, and revoking access was also tested to ensure compliance with established procedures.
* **Result**: No exceptions noted. The sample accounts were correctly assigned permissions, and the access control process was consistent with the organization’s security policies.

**Multi-Factor Authentication (MFA) Tests**

* **Tested Control**: Implementation of multi-factor authentication across all critical systems.
* **Procedure**: The configuration and implementation of MFA were verified for key systems, including EpicCare Link and TVU Networks. Tests included attempts to bypass MFA using common attack vectors such as phishing and session hijacking to evaluate the robustness of the MFA implementation.
* **Result**: MFA was found to be effectively implemented, with no vulnerabilities detected in the tested scenarios. The systems resisted common attack methods, demonstrating a strong defense against unauthorized access.

**Encryption Tests**

* **Tested Control**: Encryption of data at rest and in transit within Oracle SQL databases and Azure cloud storage.
* **Procedure**: The encryption configurations were reviewed, focusing on the application of AES-256 encryption for data at rest and TLS 1.2 or higher for data in transit. Sampled data files were analyzed to confirm encryption was applied correctly, and data transmission between systems was tested to ensure encryption was consistently maintained.
* **Result**: No exceptions noted. Encryption was properly configured and applied across all relevant systems, with data protected both at rest and during transmission, in line with NIST SP 800-111 recommendations.

**Monitoring and Logging Tests**

* **Tested Control**: Audit logging and continuous monitoring for EpicCare Link, Vulcan PACS, and Oracle SQL databases.
* **Procedure**: The audit logs were inspected for completeness, accuracy, and timely review. Logs from a representative sample period were reviewed to detect any unauthorized access or unusual activities. Additionally, the effectiveness of continuous monitoring tools like Crowdstrike Endpoint Protection was tested by simulating various threat scenarios.
* **Result**: No exceptions noted. Audit logs were comprehensive and accurately recorded all access and modification actions. Continuous monitoring systems effectively detected and responded to simulated threats, ensuring robust protection against potential security incidents.

**Incident Response Tests**

* **Tested Control**: Ransomware response plan and incident response procedures.
* **Procedure**: The hospital’s ransomware response plan was reviewed, focusing on detection, containment, and recovery processes. A simulated ransomware attack was conducted to assess the effectiveness of the response, including data recovery from backups and communication with stakeholders.
* **Result**: The response plan was executed effectively, with minimal disruption to operations. Data recovery was successful, and communication protocols were followed, demonstrating the hospital’s readiness to handle ransomware incidents.

**Confidentiality Agreement Compliance Tests**

* **Tested Control**: Employee confidentiality agreements and adherence to confidentiality policies.
* **Procedure**: A sample of employee records was reviewed to verify that confidentiality agreements were signed and acknowledged. The effectiveness of training programs designed to reinforce confidentiality practices was also evaluated.
* **Result**: All employees in the sample had signed confidentiality agreements, and the training programs were found to be effective in raising awareness of confidentiality obligations. No gaps were identified in the process.

These tests confirm that The Heart Hospital has implemented effective controls to ensure the security and confidentiality of its IT systems. The controls were found to be operating as intended, providing reasonable assurance that the hospital's service commitments and system requirements are being met in line with the trust service criteria.

**11. Identified Risks and Findings**

**Ransomware Attacks**

* **Risk**: Ransomware remains a significant threat, particularly during critical operational periods, such as EPIC go-live events, where system changes and heightened activity increase vulnerability.
* **Finding**: The hospital’s current ransomware response plan is comprehensive and effectively mitigated the simulated attack during testing. However, ongoing refinement of the plan is recommended to ensure swift recovery across all systems, particularly focusing on increasing the frequency and realism of drills to better prepare staff for a potential real-world attack.

**Insider Threats**

* **Risk**: Insider threats, including unauthorized access or misuse of patient data by employees, are an ongoing concern, particularly in a healthcare setting where sensitive information is routinely accessed.
* **Finding**: The current monitoring tools successfully detected unusual access patterns during testing, but there is room for enhancement. The hospital should consider integrating more advanced analytics and machine learning techniques to better predict and identify insider threats before they manifest. Additionally, increasing the frequency of access audits could further reduce the risk.

**Data Breaches**

* **Risk**: The confidentiality of patient data is at risk from external threats such as hacking and phishing attacks, as well as from potential internal data breaches.
* **Finding**: Encryption protocols for both data at rest and in transit were found to be robust during testing, with no exceptions noted. However, additional staff training on phishing prevention and regular updates to encryption standards could further reduce the risk of data breaches. Given the evolving nature of cyber threats, the hospital should periodically review and update its encryption methods to ensure they remain aligned with industry best practices.

**System Misconfigurations**

* **Risk**: Misconfigurations in the hospital’s IT systems could lead to vulnerabilities that may be exploited by external attackers or result in unintended data exposure.
* **Finding**: The audit revealed that system configurations were generally well-maintained, but there were isolated instances where default settings had not been properly secured, particularly in non-critical systems. Regular configuration audits and more stringent configuration management policies are recommended to ensure all systems are securely configured.

**12. Recommendations**

**Enhancing Insider Threat Detection**

* **Recommendation**: Implement more advanced monitoring tools that utilize behavioral analytics and machine learning to identify potential insider threats more effectively. Regularly update and test these tools to ensure they can adapt to new threat vectors. Increasing the frequency of access audits will also help identify any unauthorized access more quickly.

**Improving Ransomware Response**

* **Recommendation**: Review and update the hospital’s ransomware response plan, with a focus on incorporating more frequent and realistic simulation exercises. Ensure that all systems, particularly less frequently used ones, are included in the backup and recovery drills. This will help to minimize disruption in the event of an actual attack and improve overall system resilience.

**Strengthening Data Encryption and Confidentiality**

* **Recommendation**: While current encryption practices are robust, the hospital should consider adopting even more advanced encryption protocols, particularly as new technologies emerge. Regular training sessions focused on phishing prevention should be mandatory for all staff, with updates to address the latest threats and tactics used by attackers.

**Addressing System Misconfigurations**

* **Recommendation**: Conduct more frequent and thorough configuration audits across all systems, with a particular focus on ensuring that default settings are properly secured. The hospital should also enhance its configuration management policies to include regular reviews and updates to all system configurations, ensuring they meet the latest security standards.

**13. Vendor Security Assessment Integration**

The integration of vendor security assessments into The Heart Hospital’s overall risk management strategy is crucial for maintaining a robust security posture. Given the hospital’s reliance on third-party vendors for critical services, it is essential to ensure that these vendors adhere to the same high standards of security and confidentiality as the hospital itself.

**Vendor Security Assessment Process**  
The hospital conducts thorough security assessments for all third-party vendors, both during the initial selection process and on an ongoing basis. These assessments include reviews of the vendor’s security policies, practices, and compliance with relevant regulations. The findings from these assessments are integrated into the hospital’s overall risk management strategy, ensuring that any identified risks are mitigated promptly.

**Continuous Monitoring of Vendor Compliance**  
In addition to initial assessments, the hospital regularly monitors its vendors to ensure continued compliance with security requirements. This includes periodic audits, reviews of vendor security incidents, and ongoing communication to address any emerging risks. By maintaining close oversight of vendor security practices, the hospital can better protect its systems and patient data from external threats.

**14. Training and Awareness Initiatives**

A key component of The Heart Hospital’s security strategy is the implementation of comprehensive training and awareness initiatives. These initiatives are designed to ensure that all staff members are aware of their responsibilities regarding the protection of patient data and the importance of maintaining a secure working environment.

**New Hire Onboarding Training**  
All new employees undergo mandatory security training as part of their onboarding process. This training covers the hospital’s security policies, best practices for data protection, and the importance of complying with confidentiality agreements. By educating new hires from the outset, the hospital fosters a culture of security awareness.

**Ongoing Security Awareness Training**  
In addition to onboarding training, the hospital deploys bi-annual security awareness training to all staff members. This training is regularly updated to reflect the latest threats and security best practices, ensuring that employees are equipped to identify and respond to potential security incidents. Completion of this training is tracked, and employees who fail to complete the training are subject to follow-up actions to ensure compliance.

**Specialized Training for IT and Security Staff**  
IT and security staff receive specialized training on advanced security topics, including threat detection, incident response, and the use of security tools. This training ensures that the hospital’s security team is equipped with the knowledge and skills necessary to protect the hospital’s systems and respond effectively to security incidents.

**15. Conclusion**

The Heart Hospital has established a robust framework of controls to ensure the security and confidentiality of its IT systems. However, there are opportunities for improvement, particularly in enhancing insider threat detection, refining the ransomware response plan, and strengthening encryption methods. By addressing these areas and continuing to integrate vendor security assessments and comprehensive training initiatives, the hospital can further protect its systems and patient data against evolving threats.

**16. References**

* American Institute of Certified Public Accountants. (n.d.). *SOC 2® Guide Reporting on Controls at a Service Organization*. AICPA. Retrieved from [AICPA SOC 2 Guide](https://www.aicpa.org)
* CISA. (n.d.). *Healthcare and Public Health Cybersecurity*. Cybersecurity and Infrastructure Security Agency. Retrieved from <https://www.cisa.gov/topics/cybersecurity-best-practices/healthcare>
* National Institute of Standards and Technology. (2007). *Guide to Storage Encryption Technologies for End User Devices* (NIST SP 800-111). U.S. Department of Commerce. Retrieved from <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf>
* Lockheed Martin. (2023). *Proactive Measures to Mitigate the Threat of Ransomware*. Lockheed Martin. Retrieved from <https://www.lockheedmartin.com/en-us/suppliers/news/features/2023/cybersecurity-ransomware.html>
* Common Criteria Portal. (n.d.). *Common Criteria for Information Technology Security Evaluation*. Common Criteria Portal. Retrieved from <https://www.commoncriteriaportal.org/cc/index.cfm>

Thank you for your investment of time  
in looking through this SOC 2 audit.

For further demonstrations of my SOC 2 auditing experience, including additional SOC 2 audit samples, security assessment tools, and compliance resources, please visit my GitHub repository: <https://github.com/Cameron-K03/Security-Auditing>

[A qr code on a white background

Description automatically generated](https://github.com/Cameron-K03/Security-Auditing)