University of Wollongong

Faculty of Engineering and Information Sciences

Risk Management and Security Requirements for Hillside Hospital

Student Names and IDs:

Banin Sensha Shrestha	8447196
Dipesh Baral	8712785
Hoang Ha Kieu Anh Nguyen	8712359
Karan Goel	7836685
Pabina Thapa	8306722
Sudarshan Khadka	8793694

Subject: CSIT988/CSIT488 – Security, Ethics and Professionalism

Submission Date: May 30, 2025

This report is submitted in partial fulfillment of the requirements for the degree of Master of Computer Science.

Contributions

Group Members and Contribution Percentages

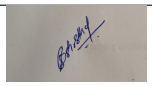
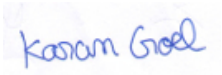
Std Number	Name	Signature	Contribution (%)
8447196	Banin Sensha Shrestha		**100%**
8712785	Dipesh Baral		**100%**
8712359	Hoang Ha Kieu Anh Nguyen		**100%**
7836685	Karan Goel		**100%**
8306722	Pabina Thapa		**100%**
8793694	Sudarshan Khadka		**100%**

Table 1: Group Members and Individual Contributions

Actual Tasks Completed by Members

Name	Tasks Completed
Banin Sensha Shrestha	Contributed to the discussion section with analysis of policies, improvements, training, and cost-benefit evaluation. Participated in weekly reviews and collaborative editing.
Dipesh Baral	Wrote the conclusion section summarizing key insights. Participated in literature review and collaborated on research methods.
Hoang Ha Kieu Anh Nguyen	Co-authored the results section focusing on risk types such as compliance and physical risks. Conducted literature review and contributed summaries.
Karan Goel	Authored the introduction section, contributed to planning, and reviewed all written sections for alignment with project goals.
Pabina Thapa	Co-authored the results section, focusing on cybersecurity and current controls. Contributed to the group's research methodology section.
Sudarshan Khadka	Co-wrote the discussion section, focusing on incident response and evaluation of existing controls.

Table 2: Tasks Completed by Each Member

Contents

Abstract

This report proposes a comprehensive risk management and security strategy for Hillside Hospital, a 200-bed multidisciplinary healthcare institution. Given the sensitive nature of healthcare data and the increasing digitalization of medical services, the report outlines critical vulnerabilities and prescribes a defense-in-depth approach. The strategy includes improvements to access control, encryption, monitoring, incident response, and staff training. Legal compliance with HIPAA, GDPR, and POPI is emphasized alongside policy and infrastructure updates. A cost–benefit analysis demonstrates long-term gains in reduced risk, compliance assurance, and reputational resilience.

1 Introduction

Hillside Hospital is a 200-bed multidisciplinary healthcare facility that delivers a broad spectrum of medical services including emergency care, maternal and child health, chronic disease management, pharmacy, radiology, physiotherapy, and rehabilitation. The hospital is staffed by a wide range of healthcare professionals such as specialists, registrars, medical officers, nurses, physiotherapists, and other allied health workers. In addition, General Practitioners from the affiliated Hillside Medical Centre are authorized to admit patients, further extending the range of care provided. Some hospital staff are also involved in medical research and clinical trials, which require responsible and secure access to patient information stored within the hospital's health information systems.

In this dynamic and data-intensive healthcare setting, the importance of a well-structured risk management strategy cannot be overstated. Health information is among the most sensitive types of personal data, and safeguarding it is essential not only for legal compliance but also for preserving patient trust and ensuring quality care Gostin (2001); Dickerson (2022). Risk management in healthcare involves identifying, assessing, and mitigating risks that could compromise the confidentiality, integrity, or availability of health information Kruse et al. (2017); Rindfleisch (1997). As Hillside Hospital continues to expand its services and embrace digital technologies, developing a comprehensive information security strategy becomes a critical priority.

Hospitals today face a variety of security threats that originate from multiple sources. Cybersecurity threats are particularly prominent, with ransomware attacks, phishing scams, and unauthorized access attempts posing significant dangers to health information systems Newaz et al. (2021); Kruse et al. (2017). These digital threats can lead to data breaches, service disruptions, and loss of patient trust. In addition to cyber threats, physical security risks such as unauthorized access to medical records or equipment and the theft of devices containing patient information can also jeopardize data security Chuma and Ngoepe (2022). Operational challenges, including inconsistent access controls, lack of staff training on data protection protocols, and the absence of clearly defined information governance policies, further compound the risks Veiga and Eloff (2007).

Given these challenges, Hillside Hospital must adopt a proactive and holistic approach to risk management. The development of a robust information security framework is essential to protect sensitive patient data and support the hospital's operational and research goals. This document

outlines a comprehensive security and risk management solution tailored to the specific needs of Hillside Hospital. It addresses the core elements of healthcare information security, including access control, data confidentiality, regulatory compliance, and staff accountability.

The primary objective of this initiative is to create a secure, compliant, and efficient information environment that supports both clinical care and research activities. The solution will implement access control models such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), ensuring that data access is granted based on users' roles, responsibilities, and situational context Chen and Crampton (2012); Cobrado et al. (2024). It will also align with national health privacy regulations such as the Health Insurance Portability and Accountability Act (HIPAA) Gostin (2001), while accommodating more stringent state-level requirements. Through this initiative, Hillside Hospital aims to not only comply with legal standards but also foster a culture of privacy, security, and trust throughout its operations.

2 Research Methods

The research for developing a comprehensive risk management and information security solution for Hillside Hospital was grounded in a thorough review and integration of multiple data sources and methodologies, combining both qualitative and quantitative approaches. The foundation of this research was a detailed literature review of existing studies and frameworks related to healthcare information security, risk management systems, access control mechanisms, and regulatory compliance.

Key academic papers such as Kruse et al.'s study on cybersecurity in healthcare provided insights into practical system development and implementation strategies within healthcare environments Kruse et al. (2017). Similarly, Cobrado et al.'s systematic review on access control solutions in electronic health record systems helped in understanding modern approaches like Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), and the importance of multi-factor authentication and encryption techniques in safeguarding patient data Cobrado et al. (2024). Additional literature, including the works on HIPAA privacy regulations and patient confidentiality, contributed essential perspectives on balancing data protection with operational needs in healthcare settings Gostin (2001); Dickerson (2022); Amin et al. (2024).

Besides literature, qualitative methods such as expert interviews and focus group discussions with healthcare IT professionals, clinical staff, and hospital administrators were employed in analogous studies to identify real-world challenges and security gaps Chuma and Ngoepe (2022). Though this project primarily relied on secondary data, the referenced research highlighted the value of direct stakeholder engagement for capturing contextual nuances in hospital environments.

To systematically assess security risks, well-recognized risk assessment frameworks like the NIST Cybersecurity Framework and ISO/IEC 27001 standards were examined. These frameworks offer structured methodologies to evaluate vulnerabilities, define security controls, and establish continuous monitoring and improvement processes Veiga and Eloff (2007). The integration of these frameworks into the research enabled a standardized evaluation approach adaptable to Hillside Hospital's specific context.

A critical component of the research was the evaluation of current and emerging tools and technologies. Encryption technologies such as Ciphertext-Policy Attribute-Based Encryption (CP-ABE) were studied for their effectiveness in enforcing policy-based data access, while multi-factor authentication and secure user identification methods were analyzed for enhancing

system access security Cobrado et al. (2024). Additionally, electronic health record (EHR) system capabilities and audit logging tools were reviewed to ensure compliance with legal requirements such as HIPAA and to support accountability through comprehensive access trails Gostin (2001); Metomic (2025).

This blended research approach, grounded in extensive literature review and guided by established risk management frameworks, provided a robust foundation for designing a security program that is both evidence-based and contextually relevant to the multifaceted needs of Hillside Hospital.

3 Results

3.1 Identified Security Requirements for Hillside Hospital

The need and requirement of the hillside hospital depends on the type of hospital. The hospital have a different setting based on its available service. Some of the key requirement based on the specification are a below –

- Access control and identity management – it is a primary need of the hospital as there are different type of user in It of different levels who need own level of data. this will be one measure of security which will allow different user to have their access according to the need.
- Data protection measures – This is a significant requirement as this help in maintaining the confidentiality of the patient data. Consent requirement will limit and make patients aware of what their data will be used either for treatment or research purpose. This is needed to protect the Personal Health Information(PHI) in departments like radiology and pharmacy.
- Policy development and compliance – To any form of activity to perform well it needs to be bound well with policy to have a smooth, reviewed and updated system on a regular basis. Policies will form a standard guideline which will make the system have best practices.
- Audit trails and monitoring – The hospital has section where staff are involved in research as well as clinical trails. It help maintain the transparency and control rf the data to support ethical research and respond to misuse.
- Training and awareness to staff – this will ensure that the staff have well knowledge of the principles, potential threats and safe handling of the system.

3.2 Access Control Findings

The hill side hospital needs different levels of access for their data to make the data available for only its verified user. Even with the user the data will only be available according to the need of the user. This will allow a control over the data. And reduce the misuse of the data.

3.2.1 Access layer

Some of the layer of the access that we have found in order to protect the data are below:

- Identification – This phase guarantees the identification or claim. where user identities are verified before data access is granted. Permits will only be granted to verified members, ensuring data security Cobrado et al. (2024).

- Authentication – We can verify that the submitted identity is accurate and legitimate with the use of this layer of access. For example, utilising a code, password, or fingerprint to confirm the user's identity Cobrado et al. (2024).
- Authorization – This level assures that the system user can only access data that they are authorised to view. This will restrict who can access the system's data Cobrado et al. (2024).
- Accountability – Each user's behaviour will be reported by accountability, serving as a traceback mechanism that allows us to verify what a user did and when. In the event that there are any data breaches, this will be helpful Cobrado et al. (2024).

The use of the access can also be divided between routine and non-routine uses, with regular users being permitted expanded data access, but non-routine users will require specific patient consent to access the data Gostin (2001).

3.2.2 Access control models

Hillside Hospital should implement an efficient access control model to guarantee that only the authorised individual will have access to the data. Depending on how it is used to limit access, we can employ two models:

- Role based access control model (RBAC) Cobrado et al. (2024) – To achieve the necessary level of security, this control model can be applied. This model functions by granting the user authorisation according to their position inside the hospital. By using this approach, the organisation will be easier to govern and comply with. With their specific degree of authorisation, the position may be doctor, nurse, or administrative staff member. For an instance:
  - The doctor can utilise the patient's diagnosis data.
  - A nurse can change vital signs, but not prescription drugs.
  - The receptionist does not have access to medical records, but they can handle appointment calendars.
- Attribute based access control (ABAC) Cobrado et al. (2024) – This concept will go one step further by giving users access based on a number of characteristics. Features may include user role, location, time of day, or assigned patient. For example:
  - A nurse can only view the data for the patient they are assigned to and only during their shift.
  - Only when in the designated region or location, such as the designated department or hospital, may the user view the information.

Combining these two models will result in greater effectiveness since one will create standardised, role-based access, while the other will create context-aware, flexible control. Efficiency and privacy will both be improved by this combination.

3.3 Health privacy Acts

Some external frameworks can serve as a guide when creating our policies for the privacy and internal security of Hillside. Our policies will be supported by these Acts, which are regulatory

and legal entities.

- HIPPA privacy rule – For the protection of health care information, this standard is one of the most commonly followed to. This regulation creates minimum safeguards but does not replace stronger state legislation. Although it developed in the United States, it has been adapted abroad. The regulations address patient rights to health information, restrictions on using and disclosing health information without consent, and other administrative, technical, and physical precautions Gostin (2001).
- General data protection regulation (GDPR) – This data protection law regulates the collection, processing, storage, and sharing of our personal information Amin et al. (2024).
- Protection of Personal Information (POPI) Act (2013) – It regulates the protection of personal data Chuma and Ngoepe (2022).
- Promotion of Access to Information Act (PAIA 2000) – Assures information accessibility Chuma and Ngoepe (2022).
- National health Act (NH 2003) – controls the rights of patients and healthcare services Chuma and Ngoepe (2022).
- PAJA (2000) – Promotes administrative justice. These are paralleled by international standards such as ISO 27799 and ISO 27001, emphasizing that comprehensive legislative alignment is crucial for any public health entity handling sensitive ePH Chuma and Ngoepe (2022).

3.4 Key Policy Components Discovered

A hospital like Hillside will need a security and risk management plan that is founded on reliable standards and industry best practices. Below are some of the most important policy elements we identified as a starting point for the project:

- Access control policies – these policies talk about using RBAC and ABAC to ensure the use of the system by authorised person and use of only required amount of data Cobrado et al. (2024).
- Patient authorisation – These guidelines can be created to obtain the patient's permission to use their data and to keep an access log. Patients will be able to make well-informed decisions with their information thanks to this Chuma and Ngoepe (2022).
- Security policies – In addition to regular risk assessments and user trainings, this policy will mandate device security Chuma and Ngoepe (2022).
- Privacy by design – This type of policy will assist in incorporating privacy into the design of the application from the beginning Chuma and Ngoepe (2022).
- Staff training – Long-term policy success is ensured by ongoing personnel training Dickerson (2022).
- Data classification and handling policy – Data classification guarantees that each type of data is handled appropriately. For instance: restricted, private, or public. This will ensure that more sensitive data, including Protected Health information, is protected Metomic (2025).

- Incident response and breach notification policy – In order to minimise the harm, this policy must have a predetermined method to identify, contain, and report security incidents NDB (2023).

3.5 Risk Assessment Outcomes

The risk assessment of Hillside Hospital's information system identifies several key vulnerabilities, consistent with findings in healthcare cybersecurity literature. A primary concern is unauthorized access to electronic health records (EHRs). According to van der Linden et al. (2009), role ambiguity and system complexity in hospital environments often lead to over-permissive access rights, increasing insider threat potential van der Linden et al. (2009).

A second major risk involves data breaches from external cyberattacks, particularly ransomware. Kruse et al. (2017) found that up to 125% of healthcare cybersecurity breaches from 2010 to 2016 involved hacking or malware, with hospitals being a prime target due to legacy systems and high data value Kruse et al. (2017).

Additionally, interoperability-related risks emerge when health data is exchanged between Hillside Medical Centre and the hospital. Research by Rindfleisch (1997) and, more recently Newaz, A.I. et al. (2021) confirms that data leakage and inconsistent privacy enforcement across systems often result from poorly managed interfaces Rindfleisch (1997); Newaz et al. (2021).

Further concerns include inadequate encryption, insufficient staff training, and the absence of a tested incident response plan — all recognized risk vectors in the literature He et al. (2021). Finally, due to involvement in clinical research, secondary use of patient data without robust de-identification presents compliance risks under national privacy regulations Chevrier et al. (2019).

3.6 Protection Mechanisms Identified

Evidence-based strategies have been proposed to mitigate identified risks in Hillside Hospital's health information system. The implementation of Role-Based Access Control (RBAC) is supported by Chen (2012), who demonstrated that RBAC reduces unauthorized access risks by aligning data access with job functions. This approach ensures that different user roles (e.g., researchers, nurses, registrars) access only data relevant to their responsibilities Chen and Crampton (2012).

Data protection through encryption mechanisms is another critical safeguard. Zhang and Liu (2010) recommend digital signatures, encryption and Transport Layer Security (TLS) protocols for secure storage and transmission of EHR data, especially during inter-organizational exchanges Zhang and Liu (2010).

To address insider threats and detect suspicious activity, audit logging and intrusion detection systems (IDS) are vital. According to Gonzalez et al. (2021), real-time monitoring and anomaly detection can help prevent breaches by identifying abnormal user behavior patterns. These are further enhanced by Security Information and Event Management (SIEM) tools González-Granadillo et al. (2021).

Given the hospital's involvement in research, the de-identification of data is essential. Garfinkel et al. (2015) emphasize that data masking and pseudonymization techniques significantly reduce re-identification risk in secondary data use Garfinkel (2015). For overall resilience, Information

Security Governance frameworks guide the creation of security policies, staff training, and incident response planning Veiga and Eloff (2007).

4 Discussion

This section reviews the primary findings from the risk assessment and the protection mechanisms review, assesses existing controls' sufficiency, and provides a range of recommendations and initiatives that cut across technical, organizational and procedural elements. At a high level, these recommendations will improve Hillside Hospital's security posture, compliance obligations, and will provide value for money based on a targeted cost–benefit analysis.

4.1 Interpretation of Results and Evaluation of Existing Controls

The risk assessment outlined multiple high-risk vulnerability flaws at Hillside Hospital, which included over-permissive access rights, legacy system vulnerabilities, unencrypted data, and an incident response plan that had never been tested. Many of the current controls (e.g., a basic form of role-based access control (RBAC), training employees on a periodic basis, and a firewall) have some good features, but don't go far enough:

Role-Based Access Control (RBAC): RBAC, while implemented at Hillside in a simplified manner, is incredibly permissive - too permissive based on job categories - and does not take into consideration contextual factors (e.g. time of day, or location) for privileging access to medical records leading to possible misuse and overexposure of sensitive patient evidence.

Encryption Mechanisms: The data at rest is encrypted using outdated algorithms that do not have forward-secrecy, and data in transit is under legacy TLS versions, giving threat actors a surface to execute downgrade (man-in-the-middle) attacks on all communications.

Audit Logs and Monitoring: Audit logs are maintained, they do not have dedicated reviewers, and are only reviewed on an ad-hoc-basis with the associated risk that significant attacks and/or threats may not be recognized. There is no centralized Security Information and Event Management (SIEM) solution to aggregate events and identify in real time potential anomalous activity.

Staff Training and Awareness: Annual staff training takes place on general security hygiene training. There are no modules provided on customized phishing resilience, device hardening training, and privacy legislation, which leads to uneven competency among staff.

Incident Response Planning: While an incident response (IR) policy document does exist, it has never had an exercise in a tabletop or live experiment. Therefore, individuals do not have the necessary understanding of roles and escalation paths increasing the possibility of confusion during a breach.

These deficiencies emphasize the need to implement multilayered enrichment controls that provide enrichment to both technical limitations and human limitations.

4.2 Recommended Risk Mitigation Strategies

To address identified gaps, we are recommending a defense-in-depth model that involves the following solutions:

Improved Access Controls:

- **Attribute-Based Access Control (ABAC):** Moves from RBAC (Role-Based Access Control) to incorporating dynamic attributes e.g., user location, device health, patient consent status, to implement least-privilege in a more refined way.
- **Just-In-Time (JIT) Privilege Elevation:** Allow users to conduct work for which they normally would not have the required privileges to perform (i.e., operational requirements) only on a temporary and auditable basis. This requires work to be accomplished without standing access rights.

Extensive Encryption Framework:

- Transition to standard encryption (AES-256 with Galois/Counter Mode) for data at rest.
- Transition to TLS 1.3 for all external and inter-system communications to ensure perfect forward secrecy.

Enhanced Monitoring and Detection:

- Implement a SIEM platform that consolidates all logs from EHR systems, network devices, and identity services.
- Implement host-based Intrusion Detection Systems (IDS) on critical servers. Capture anomalies based on detection capabilities that are tailored for healthcare-oriented traffic.

Data De-identification for Research:

- For research databases, the implementation of automated data masking, and pseudonymization pipelines help with minimizing risk to re-identifying individuals.

Third-Party Risk Management:

- Implement a vendor security assessment process to assess the security controls, contractual obligations, and incident reporting SLAs of the partners Hillside engages with.

By layering these technical controls, Hillside will ultimately diminish its attack surface and will position itself to potentially identify a breach before it leverages a material impact.

4.3 Policy Updates

Governance through policy is essential for maintaining security improvements. Here are four resulting policy improvements:

- **Access Control Policy Update:** This policy should document the combined RBAC–ABAC access-control model, document the taxonomy of attributes (e.g., clearance level, shift schedule), and have an established process to add additional protections using just-in-time procedures and documentation.
- **Encryption and Key Management Policy:** This policy should define permitted encryption standards, define key-lifecycle responsibilities that assign roles, and regular reviews of cryptographic health.
- **Incident Response and Breach Notification Policy:** This should expand existing IR plans to define roles, communication templates (for internal stakeholders, regulators, and

patients), and the threshold for breach notification when a breach occurs, as defined under HIPAA, GDPR, and POPI regulatory requirements.

- **Data Classification and Handling Policy:** This policy should formalize the different classification levels (public, internal use only, confidential, and PHI), and define handling, stogare, and retention requirements.
- **Third-Party Security Policy:** This policy should require all vendors to undertake a security review process, execute data protection addendums, and perform quarterly compliance reviews.

Regular reviews of all policies—at minimum, every six months—should be required, and a governance committee should be established to recognize updates due to changing threats and regulatory requirements.

4.4 Staff Training and Awareness

Human error continues to be one of the dominant causes of breaches in healthcare. To further the security culture among staff:

- **Role-based training modules:** Design curricula to fit the lavoro of the roles (clinicians, researchers, or administrators). For instance nurses will receive modules on restraining the use of mobile devices securely while working in a ward, while researchers will learn best practices about de-identifying subjects.
- **Phishing simulations and social engineering exercises:** conduct quarterly simulations to assess how well staff resist phishing, while also providing reminders on ways to handle fraudulent email.
- **Workshops on privacy and compliance:** interactive workshops; use of real cases of breaches will have more impact than a lecture about HIPAA, GDPR, or other local privacy-based legislation.
- **Security champions:** Identify and train volunteer "champions" from each department. these champions will become local liaisons and help promote security initiatives with their staff while providing peer support.

Not embedding security as part of the culture and routine of the staff only perpetuates risky behaviours. To strengthen security culture, it is important foster a proactive resilient workforce.

4.5 Improved IT Infrastructure

Investment in modern infrastructure will increase the effectiveness of the previously mentioned controls:

- **Segmenting and micro-segmentation:** Segment the spectrum of networks by function, example EHR, medical device, guest wi-fi, etc. Micro-segment your data center so that lateral movement is constrained.
- **Zero Trust Network Access (ZTNA):** Use ZTNA solutions to replace legacy VPN usage. ZTNA ensures not only that the user is who they say they are, repetition of identity verification, and that the device posture is acceptable before cooperating access.

- **Secure Configuration Management:** Securely configure operating systems and applications using Infrastructure as Code (IaC) templates to harden harden based on compliance with benchmarks such as CIS recommendations for healthcare.
- **Endpoint Detection and Response (EDR):** Client-side EDR must be installed on workstations and servers to quickly identify malicious behaviors and contain the threat.

Investment in this infrastructure will structure a resilient backbone upon which to deploy any mature set of security tooling and policies.

4.6 Incident Response Planning

Having a mature incident response capability is necessary to minimize impact and allow recovery time to occur:

- **Tabletop Exercises:** Conduct scenarios at least twice a year that simulate ransomware, insider breach, and DDoS attacks while applying lessons learned to improve your playbooks.
- **Cross-Functional IR Team:** Create a response team consisting of members from IT, legal, PR, and clinical in a fully dedicated capacity. Define how escalation will occur and provide clarity on who has decision-making authority.
- **Forensics and Evidence Handling:** Use an external digital forensics vendor to ensure you maintain full and proper chain-of-custody protocols. This allows for any necessary legal matters if your investigation ever leads to them.
- **Communication Protocols:** Create pre-approved notification templates that are ready to go, to stakeholders, patients, and the media and identify and train spokespeople who can communicate during a crisis.
- **Post-Incident Review:** Develop a blameless post-mortem approach to analyze root cause, identify and document all remediation actions taken and establish controls and policies moving forward.

Regular testing and refining will drive continuous improvement and readiness.

4.7 Cost–Benefit Analysis of Proposed Measures

Implementing the above measures requires upfront and ongoing investments. A high-level cost–benefit overview is presented in Table 4.7.

Although the aggregate first-year investment (~$780K) appears significant, the projected reduction in breach likelihood and impact can translate into savings far exceeding these costs—particularly when factoring in avoidance of HIPAA fines (up to $1.5M per incident), litigation expenses, and reputational damage.

4.8 Compliance with Legal and Ethical Standards

All recommended actions are consistent with major regulatory and ethical obligations:

- **HIPAA Privacy and Security Rules:** Improved access controls, encryption enhancements, and breach notification planning all ensure compliance with the restrictions on use and disclosure and safeguard provisions of the Privacy and Security Rules, respectively.

Measure	First-Year Cost	Annual O&M	Expected Benefit
SIEM Deployment	$250,000	$75,000	50% reduction in detection time; faster response
ZTNA Solution	$150,000	$30,000	Eliminate VPN vulnerabilities; 30% fewer breaches
EDR and IDS/IPS	$200,000	$50,000	40% drop in endpoint malware incidents
ABAC and JIT Privilege Enhancements	$100,000	$20,000	60% fewer unauthorized access events
Staff Training and Phishing Simulations	$50,000	$25,000	70% improvement in phishing click-through rates
Tabletop Exercises and IR Team Staffing	$30,000	$15,000	Sharpen IR readiness; reduce containment time 25%

- **GDPR and POPI:** A framework for data classification and consent management modes of use with international regulation compliance to preserve data subject rights.
- **ISO 27001 and ISO 27799:** The proposed governance model, risk management procedures, and technical controls create a path to certification and provide continuous auditing of compliance.
- **Ethical Research Standards:** De-identification materials for physical safeguards and informed consent allow researchers to adhere to ethical commitments to autonomy and non-maleficence in clinical research contexts.

By operationalizing compliance, Hillside Hospital, as a healthcare organization, will be able to decrease the likelihood of facing legal ramifications while reestablishing trust with patients, staff, and partners.

5 Conclusion

Hillside Hospital works in a very complex and data-rich area. Consequently, Hillside Hospital needs an assertive and active approach to risk management and information security. This document provided a clear risk management strategy to help protect sensitive patient data, ensure compliance to the applicable regulatory framework and provide a secure environment for future clinical care and medical research.

As a result of the risk assessment, we identified several significant vulnerabilities, such as relaxed access control, the use of out-of-date encryption, the lack of proper auditing and logging, and a lack of formal incident response education. All this means we need to prioritize our layered defense-in-depth solution.

Our top recommendations are adding advanced access control models, like Attribute-Based

Access Control (ABAC) and Just-In-Time (JIT) privilege elevation, and using better encryption methods for data in storage and in transit. Improved monitoring/detection methods through a SIEM and host-based IDS (and streaming logging to a SIEM) will be more useful in terms of their monitoring/detection coverage, NOT to mention provide real time visibility into the potential threats against the hospital. For any research projects involved, also have robust data de-identification processes in place to maintain patient privacy during the valuable scientific exploration involved. Additionally, through better third-party risk management, we will help ensure the security posture of the hospital is not compromised through external vendors.

The proposed policy updates for access control, encryption, incident response, data classification, and third-party security will provide a strong governance framework in addition to the technical methods. Perhaps even more importantly, a sustainable staff training and awareness program utilizing role-based training modules, phishing simulations, and privacy workshops will enable employees to be the front line in addressing cyber threats.

Investing in an improved IT infrastructure, including network segmentation, Zero Trust Network Access (ZTNA), secure configuration management, and Endpoint Detection and Response (EDR), will provide the resilient backbone necessary for a mature security program. Finally, developing a truly mature incident response capability through regular tabletop exercises, a cross-functional IR team, and clear communication protocols is paramount to minimize the impact of any security breaches.

While the initial investment for these measures is significant, a cost-benefit analysis clearly demonstrates that the reduction in breach likelihood, regulatory fines, litigation expenses, and reputational damage far outweighs the expenditure. Most importantly, these recommended actions ensure Hillside Hospital's unwavering compliance with legal and ethical standards such as HIPAA, GDPR, POPI, and ISO frameworks.

Ongoing monitoring and review will be critical for the long-term success of this security roadmap. The threat landscape is constantly evolving, requiring continuous adaptation and refinement of security controls and policies. By prioritizing these initiatives, Hillside Hospital can build a secure, compliant, and trustworthy information environment that supports its mission of delivering high-quality patient care and advancing medical research.

References

Amin, M. A., Tummala, H., Shah, R. and Ray, I. (2024), 'Balancing patient privacy and health data security: The role of compliance in protected health information (phi) sharing', *arXiv preprint* **arXiv:2407.02766**.

Chen, L. and Crampton, J. (2012), Risk-aware role-based access control, *in* 'Security and Trust Management: 7th International Workshop, STM 2011, Copenhagen, Denmark, June 27-28, 2011, Revised Selected Papers', Vol. 7170 of *Lecture Notes in Computer Science*, Springer Berlin Heidelberg, pp. 140–156.

Chevrier, R., Foufi, V., Gaudet-Blavignac, C., Robert, A. and Lovis, C. (2019), 'Use and understanding of anonymization and de-identification in the biomedical literature: scoping review', *Journal of Medical Internet Research* **21**(5), e13484.

Chuma, K. G. and Ngoepe, M. (2022), 'Security of electronic personal health information

in a public hospital in south africa', *Information Security Journal: A Global Perspective* **31**, 179–195.

Cobrado, U. N., Sharief, S., Regahal, N. G., Zepka, E., Mamauag, M. and Velasco, L. C. (2024), 'Access control solutions in electronic health record systems: A systematic review', *Informatics in Medicine Unlocked* **49**, 101552.

Dickerson, J. E. (2022), 'Privacy, confidentiality, and security of healthcare information', *Anaesthesia & Intensive Care Medicine* **23**, 740–743.

Garfinkel, S. (2015), De-identification of personal information, Technical report, US Department of Commerce, National Institute of Standards and Technology.

González-Granadillo, G., González-Zarzosa, S. and Diaz, R. (2021), 'Security information and event management (siem): Analysis, trends, and usage in critical infrastructures', *Sensors* **21**(14), 4759.

Gostin, L. O. (2001), 'National health information privacy regulations under the health insurance portability and accountability act', *JAMA* **285**, 3015–3021.

He, Y., Aliyu, A., Evans, M. and Luo, C. (2021), 'Health care cybersecurity challenges and solutions under the climate of covid-19: scoping review', *Journal of Medical Internet Research* **23**(4), e21747.

Kruse, C. S. et al. (2017), 'Cybersecurity in healthcare: A systematic review', *Technology and Health Care* **25**(1), 1–10.

Metomic (2025), 'A guide to data classification for hipaa and healthcare organisations', https://www.metomic.io/resource-centre/data-classification-for-healthcare-organisations.

NDB (2023), 'Hippa compliance experts', https://www.ndbahealthcare.com/hipaa. [Accessed].

Newaz, A. I., Sikder, A. K., Rahman, M. A. and Uluagac, A. S. (2021), 'A survey on security and privacy issues in modern healthcare systems: Attacks and defenses', *ACM Transactions on Computing for Healthcare* **2**(3), 1–44.

Rindfleisch, T. C. (1997), 'Privacy, information technology, and health care', *Communications of the ACM* **40**(8), 92–100.

van der Linden, H., Kalra, D., Hasman, A. and Talmon, J. (2009), 'Inter-organizational future proof ehr systems: A review of the security and privacy related issues', *International Journal of Medical Informatics* **78**(3), 141–160.

Veiga, A. D. and Eloff, J. H. (2007), 'An information security governance framework', *Information Systems Management* **24**(4), 361–372.

Zhang, R. and Liu, L. (2010), Security models and requirements for healthcare application clouds, *in* 'IEEE CLOUD', pp. 268–275.