ARTICLE TITLE

JOHN SMITH* & JAMES SMITH[1]

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

1 INTRODUCTION

2 SOLUTION

2.1 Planning and Policy

2.1.1 Information security requirements for healthcare environments

In a healthcare environment, information security is critical. Here are some information security requirements for healthcare environments:

PROTECT PATIENT PRIVACY AND CONFIDENTIAL INFORMATION, INCLUDING THE FOLLOWING

1. Patient's personal information: name, gender, age, date of birth, ID card information, home address (used by the hospital to mail medical records, bills and other information), telephone number.
2. Medical information: patient's past medical records, test results, current diagnosis, treatment records (e.g., drug use, related surgery, etc.), medical expenses, place of hospitalization (if hospitalization is required)

COMPLETENESS AND ACCURACY OF MEDICAL INFORMATION

1. Integrity: Medical information should be able to fully display the patient's recent diagnosis results, test reports. An index of past cases and examination reports is also listed.
2. Accuracy: An electronic medical record system is adopted to reduce errors and inaccuracies in handwritten records. Electronic medical records, test results and other medical information need to provide the relevant doctor or staff electronic signature for authentication before entering the system database. The system regularly and randomly checks medical information (such as medical records, examination results, diagnoses, prescriptions, etc.) to ensure its accuracy.

ENSURE THE AVAILABILITY OF MEDICAL INFORMATION

1. Establish a backup and recovery mechanism: Medical organizations should establish a backup and recovery mechanism, including regular backup of medical information and disaster recovery plans, to ensure the availability and security of medical information.
2. Establish disaster recovery mechanisms: Medical institutions should establish disaster recovery mechanisms, including backup data centers and communication systems, to ensure the availability and continuity of medical information.
3. Monitoring and maintenance: Medical institutions should monitor and maintain medical information systems, including regularly checking and maintaining devices, monitoring network status, and timely troubleshooting to ensure the availability and stability of medical information.

LAWS, REGULATIONS AND INDUSTRY STANDARDS Comply with relevant laws, regulations and industry standards, such as HIPAA[2], HITRUST, etc., to ensure the security and compliance of medical information.

ESTABLISH AND IMPLEMENT INFORMATION SECURITY POLICIES AND PROCEDURES Establish and implement information security policies and procedures, including access control, data protection, security training and awareness, risk management, etc.[3]

2.1.2 Plans

INCIDENT RESPONSE PLANNING (IRP)

1. Data backup plan details: The plan should include details such as the type of backup, backup storage location, backup frequency, and backup and recovery test plan. In addition, the plan should include security measures to determine the confidentiality and integrity of the backup data.

2. Disaster Recovery preparedness: The plan should describe how to respond to various types of disasters, such as natural disasters, power outages, cyber attacks, etc. The plan should include the members of the disaster recovery team, the division of tasks and responsibilities, a list of disaster recovery equipment, and the plan and results of the disaster recovery exercise.

3. Training Plan: The plan should describe training plans for disaster response and recovery plans to ensure that all relevant personnel understand their roles and responsibilities. The training plan shall include the planned training content, training method and training schedule.

4. Test plan: This plan should include the resources required for testing, the frequency of testing, and the purpose of testing. The test plan should cover all processes and systems related to disaster response and recovery to ensure their availability and effectiveness.

5. Copies of Service Agreements: The Plan should include copies of service agreements with suppliers and contractors. These protocols may include services and support related to data backup, disaster recovery, and business continuity.

6. Business continuity Plan: This plan should describe how business continuity will be ensured in the event of a disaster. The plan should include the resources required to restore the critical business processes, the priorities and timelines of the business processes, and the methodology for determining recovery goals and targets. The plan should also include a communication and coordination plan for how to manage employees, customers, suppliers and other stakeholders in the aftermath of a disaster. In addition, the plan should consider risks and obstacles that may exist during business recovery and provide strategies and plans to address these issues.

DISASTER RECOVERY PLANNING (DRP)

1. Clear division of Roles and responsibilities: The plan should clearly specify the responsibilities and responsibilities of the disaster recovery team members and various roles, including disaster recovery plan execution, system recovery, communications, personnel safety, and so on.

2. Execution of alarm list and notification of key personnel: The plan shall specify the execution method of alarm list and the process of notification of key personnel, including the type of alarm, method of notification, content of notification, frequency of notification and so on.

3. Clear identification of priorities: The plan should clearly prioritize business processes and information systems so that the most critical systems and business processes are prioritized during recovery.

4. Documentation of the disaster: The plan should document the details of the disaster event, including the time, location, type, impact, response, and so on. This information is critical to future disaster recovery planning and improvement.

5. Action steps for mitigation: The plan should include a series of action steps to minimize the impact of the disaster on the organization. These steps might include emergency resource acquisition, data backup and recovery, temporary workspace, crisis management, employee safety, and more.

6. Alternative implementation of various system components: The plan should include alternative implementations to ensure that critical business processes continue to function even if some system components are temporarily unavailable. These alternatives may include backup equipment, backup systems, cloud services, and so on.

BUSINESS CONTINUITY PLANNING (BCP) Business continuity planning (BCP) should facilitate the establishment of operations at an alternate site until Hillside Hospital is able to resume operations at its primary site or select a new primary location. BCP should include plans for relocating critical business functions and personnel, as well as ensuring the availability of essential resources, such as power and telecommunications.

2.1.3 Related Policy

In order to ensure different levels of access and protect patient confidentiality, Hillside Hospital may establish the following policies:

ACCESS CONTROL POLICY This policy specifies permissions and access control mechanisms of different access levels, including role-based access control, encryption, and passwords[4].

For access control mechanisms, authentication and authorization-based access control technologies, such as role-based access control (RBAC) and access control lists (ACLs), can be used.1 on the following page

1. Specialists: Experts can be granted access to cases, test results, and study data.

2. Registrar: The registrar may be granted access to cases, test results, basic patient information, vital signs, drug prescriptions, medical devices.

3. Nurse: The nurse may be granted access to the patient's basic information, vital signs, drug prescriptions, and medical devices.

4. Physical therapist: The physical therapist may be granted access to the patient's basic information, vital signs, and medication prescriptions.

5. General Practitioners: May grant General Practitioners access to cases, test results, basic patient information, vital signs, drug prescriptions, and medical devices.

6. Investigator: Investigators may be granted access to medical records, test results, and study data.

7. Patients: Patients can be granted access to their own medical information.

8. IT Department: IT department can be granted administrative authority over healthcare information systems.

9. Administration: The administration can be granted administrative authority over the healthcare information system.

10. Medical device provider: A medical device provider may be granted access to a medical device.

Role	Case	Test	Patient Info	Vitals	Prescription	Medical Devices	Research Data	Billing
Expert	1	1	0	0	0	0	1	0
Registered Physician	1	1	1	1	1	1	0	1
Nurse	0	0	1	1	1	1	0	0
Physical Therapist	0	0	1	1	1	0	0	0
General Practitioners	1	1	1	1	1	1	0	1
Researcher	1	1	0	0	0	0	1	0
Patient	1	1	1	1	1	0	0	1
IT Department	0	0	0	0	0	1	0	0
Management Department	0	0	0	0	0	1	0	1
Medical Device Provider	0	0	0	0	0	1	0	0

Table 1: Role permission matrix

DATA PROTECTION POLICY Hospitals should use the latest security software and firewalls to protect systems from software attacks. All employees should receive training to identify and report potential attacks.

1. Data backup and recovery policy: Data backups should be done regularly and stored in a safe location to prevent loss and damage. At the same time, formulating a data recovery policy can help timely data recovery and reduce the possibility of data loss.

2. Data encryption: Encryption can adopt different algorithms and techniques, such as symmetric encryption, asymmetric encryption, hash algorithm, etc. Encryption can be performed on both data transfer and data storage procedures to ensure that data cannot be stolen or tampered with during transmission and storage.[5]

3. Data loss prevention: Formulating data backup policies, specifying data storage locations and access permissions, and formulating data security training plans can reduce the possibility of data loss.

RISK MANAGEMENT POLICY This policy sets out how to identify, assess, and manage health information risks, including developing and implementing control measures, monitoring and reporting information security incidents, etc.

1. Human error or failure: Employees should receive training and supervision to ensure they are aware of proper information security procedures. Any behavior that violates security regulations will result in disciplinary action.

2. Sabotage or vandalism: All entrances and exits to the hospital should have security measures, such as video monitoring and access control systems, to prevent sabotage or vandalism. Any act of sabotage or vandalism will result in criminal or civil prosecution.

3. Deliberate information extortion: Hospitals should regularly back up data and retain backups to prevent ransomware attacks. Any ransomware attack will be immediately reported to law enforcement.

4. Theft: Hospitals should implement access control measures to ensure that only authorized personnel can access patient sensitive information. Any theft will be immediately reported to law enforcement.

5. Natural disasters: Hospitals should have emergency plans in place to handle the impact of natural disasters. Backup data and systems should be stored in secure locations to prevent damage from natural disasters.

6. Intellectual property compromises: Hospitals should ensure the protection of their intellectual property, such as patient data and research findings. Any infringement of intellectual property will be immediately reported to law enforcement.

7. Quality of service deviations: Hospitals should implement monitoring measures to ensure system stability and reliability, to provide high-quality services, and to promptly address any quality deviations.
8. Hardware failure or errors: Hospitals should implement scheduled maintenance and inspections of hardware equipment to ensure proper function.
9. Technological obsolescence: Hospitals should regularly evaluate technological equipment and software systems to ensure they are up to date with the latest technology, and take necessary measures to update obsolete technology.

2.2 Security Policies

2.2.1 Developing an Information Security Policy:

OBJECTIVE: To create a comprehensive information security policy for the hospital, ensuring that all employees adhere to uniform regulations.

METHODS:

1. Collect and analyze current regulations, industry standards, and best practices.
2. Write a detailed information security policy that combines the hospital's actual needs.
3. Regularly review and update the policy to adapt to the constantly changing security environment and regulatory requirements.

2.2.2 Access Control and Identity Authentication:

OBJECTIVE: To ensure that only authorized personnel can access sensitive information and systems.

METHODS:

1. Implement user role and permission management to assign appropriate access permissions to employees with different roles.
2. Use a strong password policy and multi-factor authentication to enhance account security.
3. Regularly review and update access permissions to prevent abuse and unauthorized access.

2.2.3 Data Encryption

OBJECTIVE: To protect sensitive data in storage and transmission from unauthorized access.

METHODS:

1. Select appropriate encryption technologies for sensitive data, such as TLS/SSL, AES, etc.
2. Use encrypted file systems to protect stored data.
3. Ensure data is encrypted during transmission.

2.2.4 Firewall and Intrusion Detection

OBJECTIVE: To prevent malicious attacks and unauthorized access.

METHODS:

1. Configure and update firewall rules to protect the internal network from external attacks.
2. Use intrusion detection and prevention systems (IDS/IPS) to monitor network traffic and report suspicious behavior in a timely manner.

2.2.5 Data Backup and Recovery Plan

OBJECTIVE: To ensure the safety of critical data and quickly recover from data loss or system failure.

METHODS:

1. Regularly back up critical data and keep multiple copies on reliable storage media.
2. Develop and test a data recovery plan to ensure quick recovery of data and systems in an emergency.

2.2.6 Employee Training and Security Awareness

OBJECTIVE: To increase employee security awareness and ensure they understand and comply with information security policies and procedures.

METHODS:

1. Provide regular information security training to educate employees on identifying threats such as phishing attacks, malware, etc.
2. Establish a security awareness program to encourage employees to comply with information security policies and best practices.

2.2.7 Regular Security Audit and Risk Assessment

OBJECTIVE: To identify and fix potential security vulnerabilities and mitigate risk.

METHODS:

1. Conduct regular security audits to identify and fix potential security vulnerabilities.
2. Conduct regular risk assessments to understand potential threats and take preventative measures.

2.2.8 Partner and Supplier Security Management

OBJECTIVE: To ensure data security is jointly maintained with partners and suppliers.

METHODS:

1. Sign data protection agreements with partners and suppliers to ensure compliance with relevant security regulations.
2. Regularly review the security practices of partners and suppliers.

2.2.9 Equipment Security

OBJECTIVE: To ensure medical equipment operates normally and prevent potential security risks.

METHODS:

1. Regularly inspect and maintain the security of medical equipment to ensure normal operation.
2. Develop appropriate access control policies for equipment to prevent unauthorized access and use.

2.2.10 Emergency Response Plan

OBJECTIVE: To develop and maintain a detailed emergency response plan to take action in the event of a security incident.

METHODS:

1. Develop a detailed emergency response plan to guide actions in the event of a security incident.
2. Establish a dedicated emergency response team responsiblefor handling security incidents.
3. Conduct regular emergency drills to ensure the effectiveness and feasibility of the response plan.

2.2.11 System and Software Updates

OBJECTIVE: To keep the operating system, software, and antivirus programs up-to-date to fix known security vulnerabilities.

METHODS:

1. Regularly update the operating system, software, and antivirus programs.
2. Monitor security bulletins released by software vendors and relevant organizations to understand new security threats and vulnerabilities.

2.2.12 Mobile Device Management

OBJECTIVE: To protect sensitive data on mobile devices from unauthorized access.

METHODS:

1. Implement security policies on mobile devices, such as remote wipe, device encryption, etc.
2. Limit employees from storing sensitive data on mobile devices and ensure data is properly protected.

2.2.13 Physical Security

OBJECTIVE: To protect the data center and critical facilities from unauthorized access and damage.

METHODS:

1. Implement physical access control on data centers and critical facilities, such as using access control systems.
2. Monitor important areas, such as using closed-circuit television (CCTV) cameras.

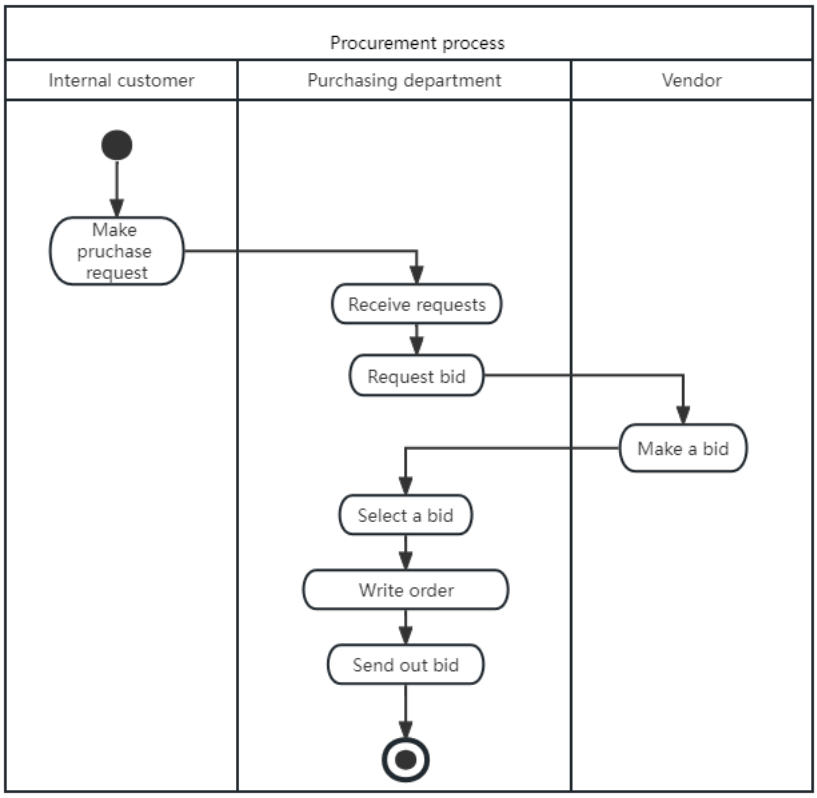

Figure 1: Procurement process

2.2.14 Security Monitoring and Log Management

OBJECTIVE: To detect and analyze abnormal behavior and identify potential security threats.

METHODS:

1. Collect and analyze security logs to identify abnormal behavior and potential security threats.
2. Retain log files for investigation in the event of a security incident.

2.3 Risk Management

2.3.1 Information Process analysis

According to this course, the first step in risk analysis is to identify processes. Based on the provided information, Hillside Hospital is a medium-sized hospital that offers a range of services, including testing, rehabilitation, emergency care, and maternity care. It also allows General Practitioners from the Hillside Medical Centre to transfer patients to the hospital. Additionally, the hospital is involved in research. Based on this, we can create the following main process activity diagrams: Procurement Process, Patient Care Process, Inpatient Admission Process, Referral Reception Process, and Research Project Registration Process.

2.3.2 system component categories

In this step, we can define the granularity of the information asset aggregation by grouping similar types of information in the hospital together. For example,

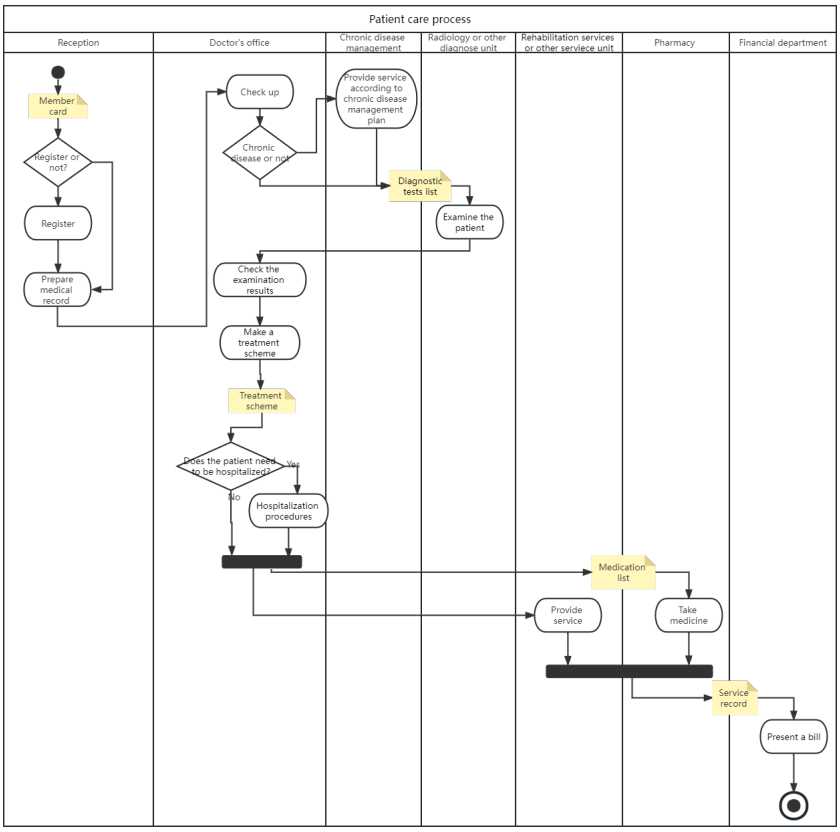

Figure 2: Patient care process

Patient Personal Identifiable Information may include full name, date of birth, social security number, medical record number, health insurance number, and so on.

Continuing with the above example, by analyzing the hospital's processes, we can hypothetically identify the following information security assets of Hillside Hospital. In this course, a classification method was presented that categorizes assets based on their confidentiality level and impact on profitability. However, in the case of hospitals, focusing solely on profitability is not appropriate. The EU standard [6] describes a classification method that divides three attributes into two levels: confidentiality - non-sensitive (C.n-s), sensitive (C.s); integrity - non-critical (I.n-c), critical (I.c); and availability - non-critical (A.n-c), critical (A.c). Classification table is shown as follows.

Information Category	Confidentiality	Integrity	Availability
Patient Personal Identifiable Information	C.s	I.c	A.c
Appointment Information	C.n-s	I.n-c	A.n-c
Payment Information	C.s	I.c	A.n-c
Patient Health Information	C.s	I.c	A.c
Hospital Financial Information	C.s	I.c	A.c
Medical Equipment Information	C.n-s	I.n-c	A.n-c
Hospital Vendor Information	C.n-s	I.n-c	A.n-c
Hospital Purchase Order Information	C.n-s	I.n-c	A.n-c
Employee Personal Information	C.s	I.c	A.c
Hospital Management and Marketing Information	C.n-s	I.n-c	A.n-c
Scientific Research Project Information	C.s	I.c	A.c

Table 2: Information Assets Classification

2.3.3 Importance List

After completing the classification, it is necessary to prioritize the information security assets according to their importance. Generally, a multidisciplinary team is needed for the evaluation, as personnel from different positions may have different perspectives on information assets. Collecting opinions from personnel with differ-

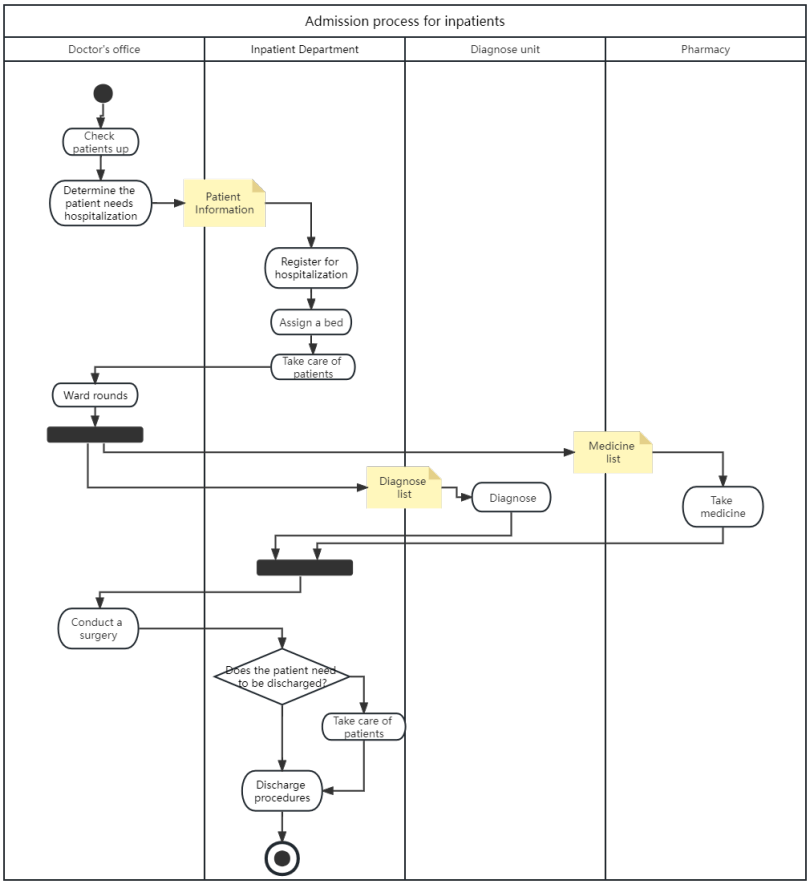

Figure 3: Admission process for inpatients

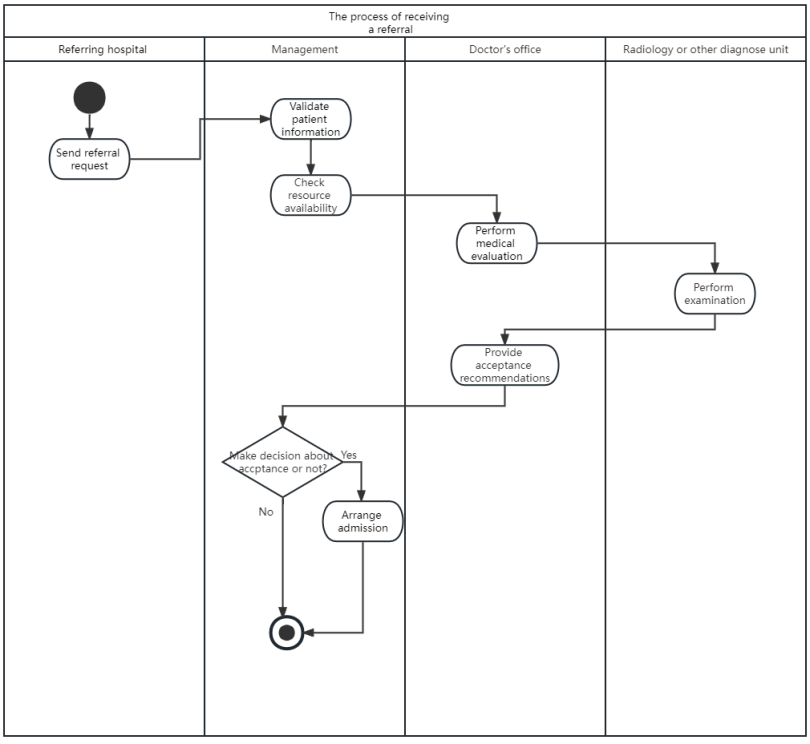

Figure 4: The process of receiving referral

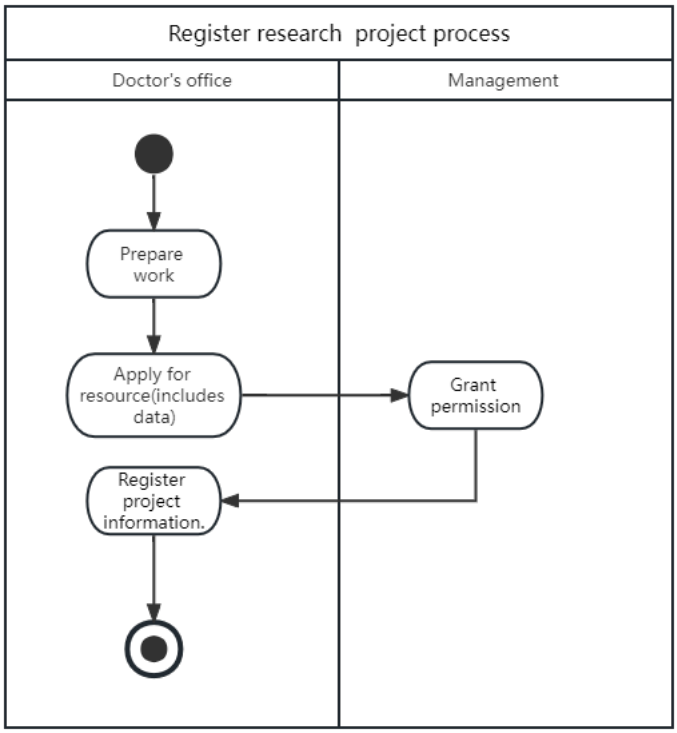

Figure 5: Register research project process

ent positions can provide a more comprehensive evaluation of information assets. For example, we consider three aspects.

Information Asset	Revenue	Profitability	Public Image	Laws and Regulation	Overall Score
Hospital Management and Marketing Information	0.8	0.9	0.4	0.4	63
Payment Information	0.8	0.4	0.7	0.6	61
Patient Health Information	0.3	0.4	0.7	0.8	55
Hospital Financial Information	0.5	0.7	0.3	0.7	54
Medical Equipment Information	0.5	0.8	0.4	0.3	52
Scientific Research Project Information	0.4	0.4	0.5	0.7	49
Patient Personal Identifiable Information	0.2	0.2	0.6	0.7	42
Appointment Information	0.5	0.3	0.4	0.4	39
Hospital Purchase Order Information	0.2	0.8	0.1	0.3	37
Employee Personal Information	0.3	0.2	0.2	0.6	30
Hospital Vendor Information	0.1	0.7	0.1	0.2	30

Table 3: Information Asset Scoring Table (Sorted)

2.3.4 Threat and Vulnerabilities Assessment

Generally, the main threats to information asset security include:[7] Now we will consider the impact of each type of threat on the different attributes of information assets.

IMPACT OF THREAT Hardware failure or errors,Human error or failure, sabotage or vandalism, and natural disasters primarily affect the integrity and availability of information assets. Espionage or trespassing primarily affects integrity and confidentiality. Hardware failure or errors, quality of service deviations and software failures or errors primarily affect availability. Theft, technological obsolescence, software attacks and deliberate acts of information extortion primarily affect confidentiality. What is particularly notable is that natural disasters, and their impact, depend on the location of Hillside Hospital. Generally, large-scale disasters pose the greatest threat to the availability of hospital information assets. For hospitals,

Threat	Possible Vulnerabilities
Human error or failure	Employee accidents and mistakes
Sabotage or vandalism	System or information destruction
Deliberate information extortion	Blackmail for disclosing information
Theft	Unauthorized confiscation of information
Natural disasters	Fire, flood, earthquake
Software attacks	Viruses, worms, and other malicious software
Intellectual property compromises	Unauthorized access to proprietary information
Espionage or trespassing	Unauthorized access for spying or intrusion
Quality of service deviations	Service provider's failure to meet expected standards
Hardware failure or errors	Equipment malfunction or failure
Software failures or errors	Bugs and code issues
Technological obsolescence	Outdated technology or systems

Table 4: Threats and Possible Vulnerabilities

among the three attributes (confidentiality, integrity, and availability), availability is considered more important than integrity and confidentiality.

To effectively manage security risks, it is essential to understand the nature and severity of potential threats. One approach to identifying and prioritizing threats is to review historical data or seek expert opinions within the relevant industry. By examining past incidents and trends, organizations can gain insights into the types of threats that are most likely to occur and the impact they may have on their operations. Additionally, seeking out the opinions of experts in the field can provide valuable insights into emerging threats or new attack methods that may not be captured by historical data. For Hillside Hospital, considering the previous analysis of the various threats, the ranking of threat severity could be as follows: Note: The extent of the threat posed by natural disasters depends on the location

Threat	Likelihood	Potential Impact	Composite Score
Deliberate information extortion	0.9	0.8	0.72
Sabotage or vandalism	0.7	0.9	0.63
Espionage or trespassing	0.6	0.7	0.42
Theft	0.7	0.6	0.42
Software attacks	0.8	0.7	0.56
Intellectual property compromises	0.6	0.8	0.48
Hardware failure or errors	0.5	0.8	0.4
Human error or failure	0.7	0.5	0.35
Software failures or errors	0.6	0.6	0.36
Quality of service deviations	0.4	0.4	0.16
Technological obsolescence	0.3	0.3	0.09
Natural disasters		0.9	0.36

Table 5: Threat rankings

of the hospital.

2.3.5 TVA diagram

Based on the previous ranking, we can create the following TVA (Threat-Vulnerability-Asset) diagram:

Asset n represents the n_th most important asset, and threat represents the n_h most severe threat. As shown in the figure, we can create six levels of control priority. Detailed controls are detailed in the Policy section and Security program section.

2.3.6 Risk Determination

FIRST METHOD In this step, it is necessary to analyze the likelihood of each vulnerability based on the hospital's historical data, the potential asset loss, the percentage of risk mitigated by current controls (referred to as mitigated risk), and uncertainty. Uncertainty refers to the accuracy derived from existing data and assumptions, calculated as 1 minus the uncertainty value.

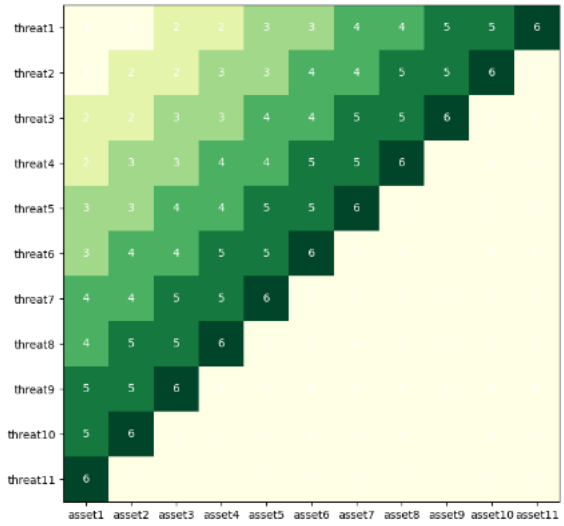

Figure 6: TVA diagram

A comprehensive score for a vulnerability can be obtained by the following formula:

$$\text{Risk Ratings} = (\text{Asset value} * \text{Likelihood}) * (1 - \text{Mitigated Risk} + \text{Uncertainty})$$

SECOND METHOD The second evaluation method is likelihood and consequence rating, which uses qualitative methods to determine the risk based on the probability of a threat occurring and the expected results of a successful attack. Based on one of the two methods above, vulnerability ratings can be obtained. The Vulnerability Risk Worksheet is created as follows:

2.3.7 Managing Risk

RISK STRATEGIES

1. Risk Avoidance: Taking measures to avoid activities or decisions that may lead to risk. The solution is to assess risks and develop plans to avoid potential dangers.
2. Risk Mitigation: Taking measures to reduce the probability and/or impact of risks. The solution includes assessing risks and implementing plans to reduce or eliminate potential risks.
3. Risk Transfer: Transferring risks to third parties, usually through forms such as purchasing insurance.
4. Risk Acceptance: This strategy assumes that the cost of dealing with risks is greater than the losses caused by risks, so doing nothing is the best choice.

2.3.8 Feasibility and Cost-Benefit Analysis

On the other hand, factors that affect the cost of a safeguard include the cost of development or acquisition of hardware, software, and services, training fees, cost of implementation, and service and maintenance costs. Asset valuation is the process of determining the financial worth of each information asset based on its characteristics and perceived value within and between organizations. This involves estimating the real and perceived costs associated with designing, developing, installing, maintaining, protecting, recovering, and defending against loss and litigation. The

Information Asset	Assets Impact	Vulnerability	Likelihood	Risk-Rating Factor
Hospital Management and Marketing Information	63	Unauthorized access to marketing strategies	0.3	18.9
		Data breach of patient feedback or surveys	0.2	12.6
		Unauthorized disclosure of strategic plans	0.1	6.3
		Insider misuse of confidential information	0.2	12.6
Payment Information	61	Unauthorized access to payment data	0.3	18.3
		Payment data interception during transmission	0.2	12.2
		Payment processing system outage	0.1	6.1
		Credit card fraud or theft	0.4	24
Patient Health Information	55	Unauthorized access to medical records	0.4	22
		Data breach during transmission	0.3	16.5
		Malware infection on healthcare systems	0.2	11
		Insider misuse or unauthorized disclosure	0.2	11
Hospital Financial Information	54	Financial data theft or unauthorized access	0.3	16.2
		Insider fraud or embezzlement	0.2	10.8
		Accounting system manipulation	0.1	5.4
		Inadequate financial controls	0.4	22
Medical Equipment Information	52	Unauthorized access to equipment settings	0.2	10.4
		Equipment malfunction or failure	0.4	21
		Inadequate equipment maintenance	0.2	10.4
		Vulnerabilities in medical device software	0.1	5.2
Scientific Research Project Information	49	Unauthorized access to research data	0.3	14.7
		Intellectual property theft or infringement	0.2	9.8
		Data breach of research findings	0.4	20
		Inadequate research data backup	0.1	4.9
Patient Personal Identifiable Information	42	Unauthorized access to patient data	0.2	8.4
		Data breach during transmission	0.2	8.4
		Insider misuse or unauthorized disclosure	0.3	12.6
		Malware infection on healthcare systems	0.4	17
Appointment Information	39	Unauthorized access to appointments	0.2	7.8
		Data corruption or loss in the appointment system	0.1	3.9
		Breach of confidentiality in appointment records	0.3	11.7
		Denial of service attacks on appointment system	0.2	7.8
Hospital Purchase Order Information	37	E-mail disruption due to hardware failure	0.1	3.7
		Lost orders due to Web server hardware failure	0.1	3.7
		Lost orders due to Web server Dos attack	0.2	7.4
		Lost orders due to software failure	0.2	7.4
Employee Personal Information	30	Unauthorized access to employee data	0.3	9
		Insider misuse or data leakage	0.3	9
		Phishing attacks targeting employees	0.1	3
		Inadequate security awareness training	0.2	6
Hospital Vendor Information	30	Unauthorized access to vendor data	0.3	9
		Compromised vendor systems or networks	0.2	6
		Lack of due diligence in vendor selection	0.1	3
		Vendor bankruptcy or discontinuation	0.4	12

Table 6: Information Asset Scoring Table

Information Asset	Vulnerability	Risk-Rating Factor	Risk control strategies
Hospital Management and Marketing Information	Unauthorized access to marketing strategies	18.9	
	Data breach of patient feedback or surveys	12.6	
	Unauthorized disclosure of strategic plans	6.3	
	Insider misuse of confidential information	12.6	
Payment Information	Unauthorized access to payment data	18.3	
	Payment data interception during transmission	12.2	
	Payment processing system outage	6.1	
	Credit card fraud or theft	24	
Patient Health Information	Unauthorized access to medical records	22	
	Data breach during transmission	16.5	
	Malware infection on healthcare systems	11	
	Insider misuse or unauthorized disclosure	11	
Hospital Financial Information	Financial data theft or unauthorized access	16.2	
	Insider fraud or embezzlement	10.8	
	Accounting system manipulation	5.4	
	Inadequate financial controls	22	
Medical Equipment Information	Unauthorized access to equipment settings	10.4	
	Equipment malfunction or failure	21	
	Inadequate equipment maintenance	10.4	
	Vulnerabilities in medical device software	5.2	
Scientific Research Project Information	Unauthorized access to research data	14.7	
	Intellectual property theft or infringement	9.8	
	Data breach of research findings	20	
	Inadequate research data backup	4.9	
Patient Personal Identifiable Information	Unauthorized access to patient data	8.4	
	Data breach during transmission	8.4	
	Insider misuse or unauthorized disclosure	12.6	
	Malware infection on healthcare systems	17	
Appointment Information	Unauthorized access to appointments	7.8	
	Data corruption or loss in the appointment system	3.9	
	Breach of confidentiality in appointment records	11.7	
	Denial of service attacks on appointment system	7.8	
Hospital Purchase Order Information	E-mail disruption due to hardware failure	3.7	
	Lost orders due to Web server hardware failure	3.7	
	Lost orders due to Web server DoS attack	7.4	
	Lost orders due to software failure	7.4	
Employee Personal Information	Unauthorized access to employee data	9	
	Insider misuse or data leakage	9	
	Phishing attacks targeting employees	3	
	Inadequate security awareness training	6	
Hospital Vendor Information	Unauthorized access to vendor data	9	
	Compromised vendor systems or networks	6	
	Lack of due diligence in vendor selection	3	
	Vendor bankruptcy or discontinuation	12	

Table 7: Vulnerabilities Risk Control Strategies Table

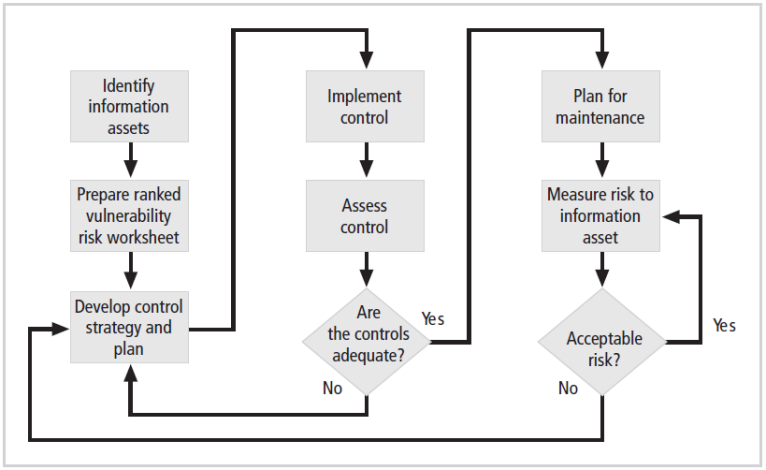

Figure 7: Risk Control cycle[1]

components of asset valuation include the value retained from creating and maintaining the information asset, value from providing the information, value acquired from protecting the information, and the value to owners and adversaries. The calculation of the value associated with the most likely loss from an attack is based on the asset value and the expected percentage of loss that would occur from a particular attack, which is usually estimated. This is expressed mathematically as the Single Loss Expectancy (SLE) where SLE = asset value (AV) x exposure factor (EF), and EF represents the percentage loss that would occur from a given vulnerability being exploited[1].

RISK RECYCLE Once the decision is made on what controls to implement, the process of risk control does not end with the design but rather requires continuous adjustment during implementation. The process of adjustment can be represented by the following diagram: The effective implementation and management of security controls is essential to achieve the identified security objectives of an organization. A control recycle approach involves implementing a specific management program that includes the consideration of funding and allocation of roles and responsibilities. This approach also involves the implementation of controls that have been selected, along with the management of operations and resources. Furthermore, it requires the implementation of procedures and other controls capable of prompt detection of and response to security incidents. By using a control recycle approach, an organization can ensure that its security controls are continuously monitored and updated as needed to address new threats and vulnerabilities. This approach can help to ensure that the organization's security objectives are met and that its assets are protected from potential security breaches.

2.4 Protection mechanism

At the forefront of our protection plan for Hillside Hospital, we prioritize the establishment of a robust access control system. This system is designed to restrict access to critical systems and valuable resources, providing a crucial layer of security in the hospital's information system. The fundamental objective here is to ensure that only users who have been granted the appropriate level of authority can gain access to sensitive information or execute specific operations.To illustrate, we can consider the case of the pharmacy staff. While their role necessitates access to certain forms of sensitive data, they should only be granted access to information directly related to medications. They must not be able to access the complete medical records of patients. This strategy of role-based access control would greatly minimize the risk

of unauthorized access or misuse of sensitive patient data.To further enhance the security measures, we propose the incorporation of strong password policies coupled with multi-factor authentication. Sandhu[8] underscored the importance of these mechanisms in their work. The combination of these two elements can significantly augment the identity verification process. It would require users to not only remember their passwords but also provide a second piece of identification, such as a security token or a biometric element, thereby adding an additional layer of security. Moreover, we advocate for a comprehensive logging system where all access activities are meticulously recorded. These logs should include details such as the user's identity, the time of access, the data accessed, and any actions taken during the session. In addition, these logs should be subjected to regular audits. Such a logging and auditing system would not only deter potential misuse but also facilitate traceability in the event of any security incidents or issues. By enabling us to quickly identify and investigate any unusual or suspicious activity, this system would contribute significantly to the overall security of Hillside Hospital's information systems.

As the second pillar of our protection mechanism strategy for Hillside Hospital, we emphasize the crucial importance of encrypting all forms of sensitive data. This encompasses not just the medical records of patients, but also extends to drug prescriptions, personal information, and any other data that could potentially be exploited if fallen into the wrong hands. Our aim is to render this data unreadable during transmission and storage, adding a significant layer of protection to the hospital's data assets. Encryption should not be a one-size-fits-all approach. To ensure the highest level of data protection, we should use robust encryption algorithms that are recognized in the field. Algorithms such as AES (Advanced Encryption Standard) or RSA (Rivest-Shamir-Adleman) have proven to be reliable and effective in preventing unauthorized users from decrypting and accessing data [9]. By implementing these algorithms, we can ensure the data is securely ciphered, making it extremely difficult, if not impossible, for unauthorized individuals to gain access. Moreover, we should look beyond just the storage of data and consider its safety during transmission. To this end, we propose the use of Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocols. These technologies create a secure, encrypted link between two points, such as a web server and a client, or a mail server and a mail client. By employing SSL or TLS, we can protect data transmission and significantly reduce the risk of data being intercepted, stolen, or tampered with during transmission. By encrypting all sensitive data, both at rest and in transit, we create a strong line of defense against potential data breaches or cyberattacks. This ensures that the privacy of patients' sensitive information is upheld, aligning with Hillside Hospital's commitment to patient confidentiality and trust.

Moreover, the hospital should deploy firewalls to prevent unauthorized access and malicious attacks from external networks. Firewalls should be set to only allow known and trusted network traffic while blocking all unknown traffic [10]. Additionally, appropriate defenses should be in place for potential internal threats.

All systems and devices should be equipped with the latest malware protection programs, and continuous security auditing and monitoring should be implemented to promptly detect and address any potential security threats. This might include real-time log recording, anomaly behavior detection, and regular system reviews [11]. Any detected abnormal behaviors should trigger immediate alerts for further investigation and handling.

The hospital should regularly provide security training and education to all staff to enhance their awareness of security risks and instruct them on how to protect patient information and adhere to the hospital's security policies [12]. Training should cover techniques to identify and avoid phishing, social engineering, and other common attacks. Strict disciplinary actions should be taken against violations of security policies to serve as a deterrent.

Lastly, the hospital should strengthen the physical security protection of key equipment and data centers. This may involve access control, video surveillance, and protective walls, among others [13]. For portable devices carrying sensitive data, such as laptops and mobile devices, strict management policies and protective measures should be implemented to prevent data loss or theft.

In summary, to ensure the system, network, data, and personal security of Hillside Hospital, we need to adopt a series of comprehensive protective measures. By implementing these Protection Mechanisms, we can effectively prevent unauthorized access, data leakage, malicious attacks, information tampering, and other security threats, thereby safeguarding the interests of the hospital and its patients.

3 DISCUSSION

4 CONCLUSION

REFERENCES

[1] Michael E Whitman and Herbert J Mattord. *Management of information security*. Cengage Learning, 2013.

[2] Health insurance portability and accountability act of 1996, 1996. Public Law 104-191.

[3] HITRUST common security framework. https://hitrustalliance.net/hitrust-csf/, 2021. Accessed: 2021-09-01.

[4] Xiaoxu Jia and Yilei Xu. A survey of access control models: Rbac and beyond. *Journal of Network and Computer Applications*, 129:1–17, 2019.

[5] Ravi Sandhu. *The RBAC model: A comprehensive review of its components, strengths, and weaknesses*, pages 1–22. Springer, New York, NY, 2015.

[6] Kees Louwerse, Margot van Ditmarsch, and Erik Flikkenschild. Experiences with a new security standard for healthcare information systems. In *Medical Informatics Europe'99*, pages 311–314. IOS Press, 1999.

[7] Michael E Whitman. Enemy at the gate: threats to information security. *Communications of the ACM*, 46(8):91–95, 2003.

[8] Ravi Sandhu, Eric J Coyne, Hal L Feinstein, and Carl E Youman. Role-based access control models. *Computer*, 29(2):38–47, 1996.

[9] Niels Ferguson and Bruce Schneier. *Practical Cryptography*. Wiley, 2003.

[10] William R Cheswick, Steven M Bellovin, and Aviel D Rubin. *Firewalls and Internet Security: Repelling the Wily Hacker*. Addison-Wesley, 2003.

[11] Karen Kent and Murugiah Souppaya. Guide to computer security log management. Special Publication 800-92, National Institute of Standards and Technology, 2006.

[12] Mikko Siponen. A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8(1):31–41, 2000.

[13] Jon Erickson. *Hacking: The Art of Exploitation*. No Starch Press, 2005.