OCTAVE Allegro Risk Assessment:
The George Washington University Hospital

Group 2
Bahareh Abrishami
Lingyi Meng
Parisa Nazarijam
Sharifa Rahmani
Yining Xie
Zhe Yang

Table of Contents

Introduction

The George Washington University Hospital (GWU Hospital) locates in Washington, DC. Since 1997, the hospital has been a partner with the George Washington University School of Medicine and Health Sciences. The hospital facility opened in late August 2002 and cost about $100 million to build, and holds approximately 400 beds with cutting-edge medical equipment worth $45 million. The building footprint is nearly 400,000 square feet (1).

The mission of The George Washington University Hospital is to promote physical and mental health in the communities it serves within Washington, DC. The hospital differentiates from other medical facilities in the District for its partnership with distinctive medical faculty of School of Medicine and Health Sciences. The organization allows the center to provide highly specialized care service using advanced technology while teaching feature physicians of tomorrow. The integrated system of academia and practice enables GW Hospital to thrive in advancing medical science through education and research continues.

GWU Hospital is aware of a variety of laws regarding the handling of personal information and their responsibility to protect customer privacy. The rules that GWU Hospital obeys include Health Insurance Portability and Accountability Act (HIPAA), Sarbanes Oxley (SOX), Gramm Leach Bliley (GLB), Payment Card Industry Data, Security Standards (PCI DSS), and Basel II, EU Principles on Privacy (4).

Information technology benefit hospitals in many aspects: efficient and faster healthcare processes, high-quality patient information, and new diagnosing and retreatment options. GWU Hospital is aware of a variety of laws regarding personal information confidentiality and their responsibility to protect customer privacy. At the same time, cyberattacks are gradually becoming more and more sophisticated, increasing the potential vulnerabilities.

Since information leaks may lead to severe adverse impacts on operations, implementing a system to secure data and information is essential for every organization. OCTAVE is an abbreviation for Operationally Critical Threat, Asset and Vulnerability Evaluation, which was developed by Carnegie Mellon University to assemble a comprehensive view of an organization 's information security needs (4).

In this paper, the OCTAVE Allegro Risk Assessment technique is used to study the George Washington University hospital for identifying risk measure criteria, developing information asset profiles, and identifying information asset containers and the areas of concern. We analysis the whole eight steps to conduct a risk mitigation plan outlining necessary measures to enhance the security level of the Hospital's staff, patients and vendors are proposed.

Step 1: Risk Measurement Criteria

The risk measurement criteria is a qualitative measurement to evaluate risk effect on an organization's mission and business objectives. Prioritizing standard set of the worksheet, Allegro requires organizational-level risk measurement criteria to reflect a range of the most significant and non-critical impact areas, which could accurately ensure that risk mitigation plans are consistent across multiple information assets. The variety of risk measurement criteria defines as high, medium, and low. The most significant risk measurement criteria for GWU Hospital are Reputation, Financial, Productivity, Safety and Health, and Investigation. The Impact Ranking Worksheet creates for ranking impact from most important to the least important in order.

Reputation (Worksheet 1): Reputation is one of the most critical areas that GWU Hospital should consider because GWU Hospital relies on technology more than ever, which may carry with a reputational risk caused by data breaches. A hospital's reputation can do much to help attract patients, qualified staff, and recommendations from referring physicians. Also, Information security problems could reduce the confidence of customers (3).

Financial (Worksheet 2): Financial benefit is the primary motivation for attackers to install and transfer malware. If the intruder goes unnoticed, significant financial harm could come to the GWU Hospital. At the same time, if economic data is inaccurate, there will be additional financial repercussions for a hospital. Even still, continual attacks against hospital network add significant delays in the reimbursement process. (2)

Productivity (Worksheet 3): For GWU Hospital, some wireless network attacks such as Denial-of-service and Man-in-the-middle would attack against hospital network and would influence hospital's ability to deliver bills to the insurance organizations electronically. There would be significant financial impacts to restore transaction if backup data missed.

Safety and Health (Worksheet 4): The public's overall perception of the GWU Hospital's quality could be negatively affected if the patient sensitive information publicize. Exposure of patient confidential information opens GWU Hospital to lawsuits and fines for breaches of HIPAA regulations (4).

.

Investigation (Worksheet 5): Critical data leaking out may result in government and other investigative organization initiatives a high profile, in-depth investigation into organizational practices.

After initial analysis of potential impact from highest to lowest level, we make the Impact Ranking Worksheet order the five Risk Measurement Criteria as following orders: 1) Financial 2) Reputation 3) Safety and Health 4) Productivity 5) Investigation.

Step 2: Information Asset Profile

Information Asset is any data, device or another component of the environment that supports activities related to information, which includes hardware, software and confidential information. However, critical information assets are essential assets of an organization and would cause enormous impact when disclosed to unauthorized personnel (7).

GWU Hospital is a complex organization that contains diversified information assets with different functions.

1) Patient's Information and Electronic Health Records: Helps to provide higher quality of service and safer care for patients while allowing for substantially improved record keeping organization.

2) Staff Information: Provides organized description of staff duties and responsibilities.

3) Facility Information: Includes track of equipment inventory, and assets' conditions.

4) Network security: Provides confidentiality, integrity and data availability.

5) Online Transaction System: Minimizes operational and shipping costs, while promoting patient engagement.

6) Medical Inventory Management System: Maintains medical supplies, equipment and other medical related items information, as well as recording how long they have stored and when they used.

7) Administrative Billing Financial Patient Registration: Provide guidance to patients on administrative side.

8) Eclectically General Ledger: Contains all the accounts for recording transactions relating to hospital's assets, liabilities, owner's equity, revenue, and expenses.

9) Image Archiving and Communication Systems: Provides a secure network to transmit patient information while allowing for economical storage, retrieval, as well as providing convenient access to images from multiple modalities such as CT and MRI.

10) Result Reporting of Laboratory and other tests: Uses the variety of mechanisms to make results readily accessible to patients and physician promptly.

Hospitals are complex organizations containing a large number of assets with different functions. We define critical holdings for GWU Hospital as assets that could have an adverse impact on GWU Hospital if any one of these assets encounters unauthorized disclosure, unauthorized modification, lost, destroy or interruption.

The most critical assets in the GWU Hospital are (1) Patient's Information and Electronic Health Records (2) Staff Information, (3) Facility Information, (4) Network Information, (5) Online Transactions System, and (6) Medical Inventory Information. Each is divided into subgroups in which each component will be considered individually to assess how each element may affect the organization security.

1) Patient's Information and Electronic Health Records

The George Washington University has an online health record system that containing medical records of individual patients. Patients can access their medical records at home or distance. They can use the online system to check: summaries of care they have received, discharge instructions, lab results, medications, health issues, allergies, immunizations, procedures, and radiology reports. (The George Washington University Website) Patients can either register online or in person with medication record numbers that were assigned to individual patients.

Electronic Health Records is a crucial part of GWU Hospital clinic section. The health record contains long-term detailed records of the individual patient and the personal information such as address and age. GWU Hospital serves patients and provides health treatment for patients, which means patients are the number one essential stakeholder. The electronic health records of patients are the crucial information assets for GWU hospital to focus. GWU hospital considers the protection of the health records as the top priority by keeping backup and having the firewall for the possible data breach.

The George Washington University Hospital has to follow HIPAA Privacy Rules because patients' personal information and medical records are sensitive information assets.

"The updated firewall is needed to protect the health record from being hacked by attackers. The GWU hospital has IT department to manage the firewall system. The IT department also monitors potential threats to keep the records safe.

The patients and doctors are not the only people who get accessed to the health records. The authorized third parties could use a large amount of health record to analyze for statistical reasons. GWU hospital has a safe access method for authorized users to use the data and not to compromise the safety of patients' electronic health records".(3)

2) Staff Information

The George Washington University Hospital employs qualified doctors, nurses, therapists, and staff (Clerical staff, Information technology staff, Food services staff, Environmental services staff, Pharmacy staff, accountants, financial officers, etc.) to provide patients with the best health services to excel in their healthcare and academic achievements. Protecting personal information of staff such as names, address, DOB, SSN, and phone number is one of the critical tasks in privacy control. There are lots of reasons why people should practice for privacy control, such as preventing identity theft, protecting employment records and insurance, and protecting SSN and banking information.

3) Facility Information

The George Washington University Hospital is the healthcare institution that has an organized medical and other professional inpatient facilities. The GW hospital owns different central centers, which provide various services for patients. The amenities include the laboratories, radiology, inpatient charts, and outpatient chart.

1. Laboratories

Blood/specimen information: the laboratory hardware reports routine patient blood reports (CBC, BMP, Lipid panel) and in some instances staff into the EHR. For example in the morning blood samples collected by the nursing staff is sent to the blood lab. There the samples are fed into the blood analysis machine and reports generated regarding the examples are sent to the EHR to be viewed by the medical staff.

Microbiology (blood cultures): If a patient suspect was having a blood infection (elevated WBC from the blood test or fever), the physician might deem necessary for the blood to be cultured so the pathogen can be identified. This can go a step further by testing the culture against a set of antibiotics at which point the physician is provided with detailed information regarding the sensitivity of the pathogen to a specific antibiotic.

Pathology (surgical specimen, biopsies): If a patient has a biopsy done (tissue sample was taken from the patient) the pathology lab investigates the origin of the tissue and report if the fabric is benign or malignant. This sample can be sent to the Microbiology lab to be cultured as well.

2. Radiology Images

All imaging reports (CT, X-ray, MRI, ultrasound) Patients often require imaging for further evaluation and diagnosis of their pathology. This can be as simple as a broken limb or as complex as a CT scan or MRI identifying a mass lesion, obstruction or internal bleeding.

3. Inpatient charts

Procedure notes, H&P, progress notes, consults, discharge summaries patient daily records of care essential to maintaining a record of the care and also a mean of communication between the medical teams of each specialty. This information will also help the outpatient management of the patient's health.

4. Outpatient chart

Visit notes, immunization reports, screening and preventative care reports (colonoscopy, mammogram, pelvic exams). These records allow for continuity of care between the care team and help the inpatient team should the patient is admitted to a hospital. ”Many differential diagnoses of an inpatient visit can be easily nulled given previous outpatient records such as immunizations or screening tests.

For each facility, it is very critical to track all the information about equipment, patients, and service conditions. Each institution depends on its security level has limited access to data which needs to providing training to those with access to the patient's information and medical data. Establishing policies and procedures for the storage of proprietary information, physical and technical control such as passwords on computers, ID badges, safeguard keys, access cards, secure doors, and cameras to control the entrance and exit of individuals from these facilities”. (3) Other data may fit into the following categories:

- Public, which is available for anyone;
- Internal freely shared and be available within the institution;
- Department shared only within the department;
- Laboratory shared just in the laboratory;
- Confidential, shared only with those directly involved with the data or on a need-to-know basis.

4) Network information

Network information is one of the most critical parts of the hospital, so is GWU Hospital. Network information security objectives are consistent with other information assurance objectives, however even more challenging. There are three kinds of parts for network information security in GWU Hospital, first is confidentiality which means protect confidential information processed, stored on and accessible from hospital networks, second is integrity, it can help people to ensure the accuracy of data transmitted, the last one is availability, it will make sure that authorized users can use the hospital network availability. A public network information is a type of information wherein anyone, namely the general public, has access and through it can connect to other Internet. This is in contrast to a private network, where restrictions and access rules are established to delegate access to a select few. Since a public network has few or no restrictions, users need to be wary of possible security risks when accessing it.

VPN is a most popular method for providing secure remote access to hospital networks. And VPN uses encryption and tunneling protocols to create a secure, private connection through a public network; it is used to ensure the confidentiality and integrity of data in transit. Doctors can connect to the GWU hospital network when they have a meeting outside to search some information in GWU hospital by VPN. It will be more secure and private than other network connection. Digitized data in healthcare is growing. Data is now processed from internal and external sources, including mobile devices, wearable sensor devices, blogs and remote health monitoring systems. Terabytes of data generated from medical sensors are also used to increase the likelihood of reliable health diagnoses through accurate and detailed real-time data analysis.

Pervasive wireless communication and computing can facilitate a variety of e-health applications to communicate patient medical data and information to the doctors/caregivers in an e-Health environment. With the advancement of medical devices and practicing methods, the concept of in-cooperating latest communication techniques has taken a new direction by enabling cognitive radio networks in e-Health applications.

5) Online Transactions Data (OTD)

Online Transactions Data (Worksheet 11) in GWU Hospital primarily contains Patient registration Data, Billing Data, General Ledger Data, Cost accounting Data, and Payroll Data. Online Transaction Data contains all the information necessary to bill a patient and insurance company for treatment or services received from GWU Hospital.

a. Patient registration data includes patient information such as Name, Address, Social Security Number and Insurance Companies

b. General Ledger Data consists of Date of Transaction, Transaction ID, Item Name and Price

c. Cost Accounting Data maintains details of Income Statement, Balance Sheet, Cash Flow, Comprehensive Statement and Statement of Change to Equity

d. Payroll Data includes critical information of faculties such as Faculty ID, Bank Account, Working period and total salary (8).

According to Payment Card Industry Data Security Standards (PCI-DSS), location and network ought to obey PCI-DSS as long as the credit card is keyed in or swiped. GWU Hospital entrusts the Atlantic CBD Web Site, an online bill service, to establish and maintain online payment authorization and process for customers. In using the services, customers are requesting Atlantic CBO to make payments from customers' designated transaction account. Atlantic CBO would not charge customer of the electronic transaction, and both of GWU Hospital and CBO obey PCI-DSS strictly. (3)

6) Medical Inventory Information

The George Washington Hospital Administration uses Inventory Management System to keep precise and updated inventory information of its medical supplies, medical equipment and assets. As medical supplies are the most used products in a hospital, the GW Hospital ensures maintaining the stock of lifesaving medicines, injections, and disposable surgical items such as syringes, masks, glove, etc. across all of its units and pharmacy.

By using inventory management system, George Washington Hospital provides its staff with real-time status and location of its medical equipment. It ensures availability and location of EKG Machines, Electrosurgical Units, Stress Systems, Diagnostic Ultrasounds, Anesthesia Machines, Surgical Instruments, etc. which are critical in providing patient care.

Step 3: Information Asset Containers

Information Asset Containers are placed where the critical asset is stored, transported, or processed. In an information security risk assessment, the identification of crucial containers is essential to identifying the risks to an information asset and to ensure that internal and external threats to an information asset are considered. Usually, Information Asset containers are supposed to emphasize three aspects: Technical Containers (Worksheet 9a), Physical Containers (Worksheet 9b), and People (Worksheet 9b)

- **Patient Health Records System**

Technical: For the patient records Database (system), the George Washington University Hospital has three different area of containers: technical, physical, and people. For the technical containers, the GWU hospital has both internal and external factors. The IT department as an internal of the organization is in charge of the daily operations of the patient records system. The department oversees the system and makes sure they are present if anything happened to the system. The external technical organization would be the company that owns the health records system. Their primary job is to provide technical support if GWU hospital cannot handle any issues related to the health records system.

Physical: The critical patients' information is stored inside the GWU hospital. Computers and database located inside the GWU hospital. The company that provides the patient records system will have the external backup of the data to protect potential risk of losing any critical data due to emergencies.

People: Patients as the most critical stakeholder of the GWU hospital is the external who will use the health records system online to access their medical information. They can access their medical records through the Internet without considering the physical distance. Another external personnel of the health record system are the company who made the system. Their employees who have access to the system and the data is the external personnel. "The internal people who have access to the system and the data will be doctors, nurses, and employees who are authorized to alter the medical records. A thorough training plan should be in place to train related employees to protect the sensitive medical information"(3) .

- **Network information**

Technical: GWU hospital network system has both internal and external parts. The internal part is the medical network service can replace or supplement some or all of an expensive internally staffed clinical facility network with a cloud-based networking service. And GWU hospital creates the wireless network in their offices and wards by many routers. The medical network service can provide these services to large existing clinical facilities such as GWU hospitals. The medical network service can increase security and reliability of those networks. Also, the medical network service can provide synergistic benefits that can improve patient outcomes and patient care. Also, a medicinal edge router can give redundant communications features for transmitting patient data to the medical network service. Extend part is that network operator such as Verizon offers the network to GWU hospital and keep it secure and regular (5).

Physical: There are some network servers in GWU hospital network server room. The medical network service in GWU hospital can provide networking services via software as a service technology, platform as a service technology, and infrastructure as a service technology. And GWU hospital will store their network information in their network server room, and network operator will also monitor the network data for GWU hospital.

People: The GWU hospital network department manager designed the hospital's network. He knows the kind of the GWU hospital network's firewall and the defense in depth. And he will not post this information on the website or to the public. People can connect the GWU hospital network or wireless network, but they will not know the details about the GWU hospital's network security.

- **Online Transaction System**

Technical:

· **Billing Management System (BMS)**: The Online Transaction Data is primarily built on the billing management system (BMS), which is considered as the container and consists of two database servers and three application servers on Windows 7(3).

· **Network**: At the same time, all online transactions across the BMS system are on GWU Hospital Internet network that is another container (4).

· **Financial Database**: GWU Hospital implements internal E-commerce information system and sensitive customer financial database to ensure the integrity, availability and confidentiality of each transaction in finance department workstations, which is also one container owned by IT department (3).

Most bills are shipped to insurance companies periodically. (4) The insurance company would be regarded as the owner of the information asset when billing information arrives, from which process the Internet turns to be the container. (Caralli, 2007)

Physical:

· **File Folders**: Partial paper receipts are stored in file folders in the file room on the third floor of GWU Hospital (3).

· **Super Server**: Paying an invoice requires information automated in Accounts Payable System and stored on the Super Server of GWU Hospital (11).

· **Backup Tapes**: At the same time, some backup data of BMS system may be stored onsite (4).

For the external physical container, paper copies of billing statements to patients, insurance providers, and banks contain critical data, which owned by Financial Staff. (Caralli, 2007)

People:

· **John Jones:** He is a director of finance in the financial records department and has authority to access to financial records and pass files around the office.

· **Amy Green**: She is the order entry staff who oversees business services for GWU Hospital (3).

· **Insurance companies and Third Parties**: For organizations outside GWU Hospital, insurance claims staff and third-party vendor managers are also critical for online transaction. Third parties such as Data Inc. manages the transportation and storage of backup tapes for the BMS system. The Hospital IT department controls the relationship.

- **Medical Inventory Information**

For Medical Inventory Information, the George Washington University Hospital has three different area of containers: technical, physical, and people.

Technical: For technical containers, the GWU hospital has both internal and external factors. Its internal factor is the Information Technology department who oversees the daily operations of the Inventory management system, which runs on various software, and hardware platforms owned by GWU hospital. Also, the hardware such as smartphones, tablets and computers on which the system run is connected through the GWU hospital network. The IT department is in charge of any technical difficulties occurring to the system. Its external container is the vendor who owns the inventory management system. They maintain the system by providing technical support.

Physical: The medical supplies and equipment information is stored in GWU hospital's server located in GWU hospital server room. The GWU hospital also keeps a backup of the data in case the data is lost or stolen.

People: The inventory management system internal users are the pharmacists, nurses, doctors, accountants, technicians and warehouse staff who are authorized to access, retrieve and manipulate information to manage the medical supplies and medical equipment. The external users are the inventory system management vendor staff that accesses the system for technical maintenance.

Step 4: Areas of Concern

Area of Concern is the statement to describe details for real situation that could influence an information asset for GWU Hospital (8). The purpose of identifying areas of concern is to frame a potential threat list for information assets.

- **Patient's Health Records System**

The major concern regarding information assets relating to patients is that the institution or hospital departments will be damaged by losing or stealing susceptible information and data of patients. If this happens, it will have a significant impact on hospital business goal in the long term. One of the areas of concerns would be disclosing information to unauthorized people or organizations. Since Doctors, nurses, and staff have access to patient's information on DBMS, intentionally or unintentionally may disclose the information. Money can be the main motive for a team to sell the data to unauthorized users, so the administrative department should consider monetary penalties for violators or filing lawsuits against people who sell confidential data. Also, training can help to minimize the human errors, which might be one of the main reasons for concerns.

Second, the risk of an outside attacker attack the database is another major concern related to the health records database. The motive for this kind of attack will be financial related. The attacker can sell sensitive medical information and personal information to an unauthorized third party. How to prevent the external attack and mitigate the risk is the critical area of concerns.

- **Staff Information**

Each patient's' key information about their medical conditions and clinical cares is recorded and stored electronically in a database which is maintained and controlled by the GW Hospital department. If the information recorded in patients' paper health record, it may also have transformed into electronic form and saved. The hospital may share information with some social care organizations for ongoing care or treatment, or the hospital is asked to share information as required by law. The database exists on a server which is maintained by the hospital and can be accessed through computers which reside within GW hospital network.

The database access is controlled for the security reasons. The database is updated by nurses and administrative staff for making necessary changes and updating patients' medical records.

- **Online Transactions System**

Online Transaction Data are extremely susceptible to fraud by insiders because of the ability to obtain money from hacking activities. At the same time, some cybercriminals have interests in gaining access to financial systems and redirect financial flows or collect passwords to communication systems such as e-mail and use them for spamming purposes. (Caralli, 2007)

1. **BMS System Vulnerability**: Billing data altered when unauthorized individual gains access to GWU Hospital BMS system. Vulnerability in the Windows 7 operating system leveraged to administrative access. If the intruder goes unnoticed, GWU Hospital will face significant monetary loss. If insurance companies were not charged correctly for services, the hospital would lose money (11).

2. **Patient's Billing Information Disclosure**: If the Patient information is disclosed to unauthorized individuals, GWU Hospital may be open to HIPAA violations and lawsuits. GWU Hospital's reputation could be negatively affected as well (8).

3. **Denial-of-service attack**: GWU Hospital network can electronically deliver bills to the insurance organizations. Continual assaults against network significantly delay transaction process.

4. **Least Privilege**: An unauthorized individual can get access from database administrator incorrectly and view BCD asset and exposes it to others, which also breaks HIPAA and results in reputation deduction (11).

5. **Incident errors**: Backup tapes lost and unable to recover transactions, which would be significant financial impacts to the transaction. At the same time, the billing statement may send to wrong patient address by fault caused by employees.

- **Network and Wireless Network**

Hackers may gain access to the GWU hospital's network and wireless network access point by eavesdropping on wireless device communications. The malicious code involves viruses, worms, Trojan horses, logic bombs, or other unwanted software that is designed to damage files or brings down a system. Theft of service occurs when an unauthorized user gains access to the network and consumes network resources. In GWU hospital's wireless networks, the espionage threat stems from the relative ease with which eavesdropping can occur on radio transmissions. Attacks resulting from these threats, if successful, place an agency's systems—and, more importantly, it's data—at risk.

- **Medical Inventory Information**

George Washington Hospital Inventory Management System contains valuable medical information assets, which is more appealing to hackers than any other data in the market. Its existence in a database on a server makes it extremely exposed and appealing target to cyber threats. Since the internal users can access the system on a variety of hardware and software platforms, they may intentionally or unintentionally expose the information to unauthorized users. Furthermore, monetary benefits and cyber warfare may attract cybercriminals to steal and sell the information to unauthorized users or tamper the information which will result in negatively damaging the GW hospital reputation and pose significant safety and legal liabilities.

Moreover, higher connectivity provides more potential attack vectors since the data saved in the system can be accessed through every computer wirelessly connected to the hospital network. In any case, there is particular concern over the vulnerabilities of the software, computers and server nearly all of which are connected to the network in some way, where the potential for patient harm is enormous.

Step 5: Identify Threat Scenarios

- **Patient Health Records Threat**

The most crucial information asset of the George Washington University Hospital is patient health records. The medical records valued the most at GWU hospital. The third party who is in charge of managing the backup of the medical files is considered as physical access. More important, the employees of GWU hospital who manage the patient health records have full access to confidential data. The employees who handle the patient health records is an actor may violate the confidentiality of the asset. The external attacks from the malicious third party is another actor, which contradict the confidentiality requirement of security. Another factor is the physical access to the patient health records. The GWU hospital could have a power outage for a period. The backup power should also keep the medical records safe and available to the users, which may violate the availability of the patient health records. The intent of the actor may both be deliberate or accidental. They may unintended or intended to disclose confidential and sensitive data to others. The outcome for the employees results in disclosure of raw data.

The external attackers have a financial motive. The issue of the attack is loss or disclosure of confidential information.

- **Staff Threat**

Nowadays, healthcare data is becoming more valuable to hackers, and hospitals are a gold mine for cyber-attacks. Every hospital staff member needs to know how to identify, analyze, and mitigate threats. Just as there are medical codes and best practices that every employee is required to learn, it's time to do the same with cybersecurity. Most of the times hospitals are amazed that one of the biggest threats to data security is their staff. The first scenario begins from exposing of doctors, nurses, and patients' information to external unauthorized entities. It may cause by their staff accidentally or intentionally because they have access to the database of patients, doctors, and nurses.

Another reason which might be the cause of this scenario is that not all staff and employees are educated about information security and cybersecurity, so sometimes uneducated staff about cybersecurity have role-based access to the database and selling, modifying or even deleting the information for money can be the motive for them. The hospital needs to have detailed data governance, risk management and data security policies in place to make sure staff are all associated with the hospital's cybersecurity strategy. Also, the hospital needs to consider preventive actions such as training staff and workers and considering the consequences of their contracts. The likelihood of this threat is low, but if it happens, the damage will be high to the hospital. First of all, they have to spend lots of money on fixing the breach. Second, the hospital reputation will be damaged, and it may be sued by doctors, nurses and patients. This risk can be mitigated by applying a few actions and policies on technical and administrative containers such as: Do not download or use the software without IT's permission or do not open emails from unknown senders.

Physical security is not directly linked to the cyber-threats. However, it cannot be neglected and let it be the cause of cyber-attacks. Physical threat is quite easy in most facilities at hospitals. Indeed, most doctors, nurses, patients' rooms offer the connection to the network as they expose open ports used for plugging medical devices. So, attackers can quickly create situations allowing them to access these network entry points. This exposure can be mitigated if the network is monitored.

"Vulnerability assessments is a process used to identify weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset. For example, an asset-based assessment at a hospital's research lab will focus on the information developed by the researchers, both from a physical security and information security perspective. In this instance, the primary asset in need of protection is the information in both its physical form (computers, paper, etc.) and its electronic form (software, files, etc.). Asset-based assessments assume that every scenario cannot be imagined or those that are, are too speculative to consider." (15)

Threat-based vulnerability assessments focus on the various kinds of threats that challenge hospital security sections. While the vulnerability assessment team's goal is to select a low-frequency threat with minimal impact for the assessment, the scenario must be adequately realistic. The training, skills, and equipment of the theoretical adversary should be considered as each protection layer is breached. Finally, the assessment team analyzes the consequences of the threat and risks, analyzing the risk, reaching its target and assigns a vulnerability rating.

- **Facility Threat**

With information being one of the most significant assets of each organization, securing data and information are as critical as preserving physical assets and equipment from being stolen, vandalized, and disturbed. The security and data breaches can have devastating impacts on organization operation; therefore, identifying the threats and vulnerabilities are on the forefront of decision makers list of priorities.

With growing incidents of cyber-attacks across the globe, many of the organizations have become more vigilant and have adopted policies and procedure to safeguard their information through implementation of information security systems. Identifying threat scenarios and preparing plans to prevent and react to each is pivotal to the implementation of security system success. All equipment and systems users should ensure that policies and measures are in place to prevent attacks aiming to steal, damage, and compromise their physical and intellectual assets. When it comes to vulnerability, George Washington University Hospital is not an exception. Therefore, it is essential for all GWU hospital staff, faculty, students, patients and visitors using GWU hospital facilities, services or IT systems to understand the need to ensure the protection of any university equipment.

- **Network Threat**

There is a growing tendency that hospital can live without the network. The network is crucial for GWU hospital; doctors need to use the network to look patient's records on their computers. And medical bill requires connecting to the network to verify the bank account information.

Nowadays internet is used on a large scale, so the phishing attacks are becoming very common. The internet has become a necessary need of the person. The phishing attacks can globally acquire the user's confidential information like username, credit card number, and password, etc. And this data may be stored on to the database and may be used for the illegal purposes. Phishing is the attack mainly done to gain access to confidential information of the victims.

As the year's progress, the cyber landscape remains in a constant battle of attack and defend. Unfortunately, the attacker holds the advantage with dozens, if not, hundreds, of different ways in which hospital is susceptible to attack. The defender has the overriding goal of defending the entire technology stack and plugging any hole in the security of GWU hospital, which is nigh impossible with the slew of zero-days lacking secure coding practices. Notably, one of the greatest strengths and weaknesses of hospital's security posture is the human element. An employee properly educated in cyber-attacks and suitably restricted from critical systems can be a tremendous asset to the defense posture of the hospital, often recognizing and reporting attempted attacks before any damage occurs. Contrast that to untrained individuals that will immediately click a malicious URL, browse to suspicious websites, or enable that script to run in a weaponized document (16). Attackers are well-aware that humans are susceptible to these types of attacks and as before-mentioned, it continues to be the number one initial vector for intrusions.

- **Online Transaction Data Threat**

A threat to Online Transaction Data is an indication of a potential undesirable event, a situation in which a person could do something obnoxious, or a natural occurrence could cause an adverse outcome. When a threat actor exploits a vulnerability in OTD, a threat is created. A threat scenario refers to a situation in which an information asset can be compromised, which is a simplified way to determine if a risk exists that could affect your information asset. A threat scenario consists of an actor, a motive, a means and an undesired outcome.

- Asset is something of value to the GWU Hospital
- Means refers to the way that the actor accesses the asset.
- Actor indicates the person who may violate the security requirements of an asset.
- Motive is the intent of an actor
- Outcome equals to the immediate result of breaking the security requirements of an asset.

The threat tree is used to visually represent a range of threat scenarios to help GWU Hospital to ensure a broad range of potential threats to Online Transaction Data. Our team represent Threat Tree in Table 4

Table 4: Threat Trees for Online Transaction Data

Threat Tree	**Definition**
Physical means by Human Actors	The threats in this category represent threats to Online Transaction Data via the GWU Hospital's technical access a File Folders, Super server or Backup Tapes that host an Online Transaction Data deliberately or accidentally.
Technical access By Human Actor	The threats caused by BMS, Network, Financial Data to a container that hosts Online Transaction Data. A personnel requires direct action deliberately or accidentally.
Technical problems	GWU Hospital's information technology and systems cause this problem containing hardware defects and software defects.
Other problems	Problems are beyond the control of GWU Hospital. This category of threats includes natural disasters and unavailability of infrastructures.

- **Medical Inventory Information Threat**

In the current environment of rapidly evolving types of attacks, hospitals are prone to many kinds of threats to their information assets. Although a robust consideration of possible risks to George Washington Hospital is hard to provide. One threat scenario is people external to George Washington Hospital can exploit technological vulnerabilities of the application to conduct denial of service attack and interrupt access to Medical Inventory Management System. The hospital is dependent on medical inventory information to function properly. Thus it is rendered helpless without it. Disruptions to Medical Inventory Management System can affect the hospital's ability to provide the patient's' immediate prescription and treat the patients. Eventually, this can affect the health of the patients, resulting in lawsuits, and altering the reputation of the hospital.

Another worrisome threat scenario is internal dissatisfied authorized staff or users of the system who could use their access to the Medical Inventory Management System to modify patient medication deliberately. A patient's life and health could be affected due to improper changes to the drug resulting in lawsuits which will lead to damaging the hospital's reputation.

Step 6: Identify Risks

- **Patient Health Records Identify Risks**

The employees of GWU hospital need to go through proper training. They have to know the patient health records system to mitigate the chance of misuse or unintended disclosure of sensitive information. The employees should pay attention to possible risk factors and alert related managers if they found any identified risks.

- **Staff Risks**

Risk identification is the process which each staff member at hospital and healthcare employees become aware of the risks at the hospital environment. Risks to doctors, nurses, and staff are dominant at hospitals. Thus, it is essential for the hospital to have a very highly qualified healthcare risk managers to assess, develop, implement, and monitor risk management plans with the goal of minimizing the threats. Hospitals have many priorities such as finance, safety and most importantly, patient care.

Identifying and evaluating risks helps staff, and managers reduce injury to patients, staff members, and assets at the hospital. Potential risks have to be analyzed and measured regarding their potential impact which might have on the business mission. "The threats of not preparing for potential risks at the hospital can have a significant, and long-term impact. Neglecting to have comprehensive risk management plans in place can compromise patient care, increase liability risks, and result in financial losses." [17]

- **Facility Risks**

Identifying risks include establishing a baseline to avert interruption, loss, damage or compromise of GWU hospital physical and informational assets, preventing adverse impacts to the facility operation. Following security guidelines, controlling access to laboratories and test facilities, maintaining assets inventory are few examples are preventive measures to mitigate the risks.

- **Network Risks**

Attackers can attack GWU hospital's network room or operator's network room in physical or virtual ways. For example, attackers can explore the electric power about GWU hospital; then the network room cannot work. Attackers also can attack GWU hospital's website by DDOS; it's a very useful way for attackers to attack the target.

- **Online Transaction Data Risks**

The risk for OTD, composed of event, consequence and uncertainty, refers to a person or a natural occurrence could cause an undesirable outcome, resulting in an adverse effect or value for GWU Hospital's OTD. Usually, the addition of threat and impact is equal to risk. Our team analysis how the threat scenario could impact the Online Transaction Data of GWU Hospital specifically.

Threat Scenario	**Consequence**
Incorrect database permissions enable personnel to access online transaction records accidentally.	The online transaction records of an employee are disclosed, resulting in a lawsuit filed against the GWU Hospital
John Smith is the only employee who knows keyword to manage online transaction database. If John Smith leaves the company, GWU Hospital cannot access the Database.	Online Transaction Database is not produced, resulting in loss of production revenue of $255,000 per day.
An unauthorized employee alters a patient's online transaction records.	An incorrect online transaction is given to a customer, resulting in GWU Hospital's reputation damage.

- **Medical Inventory Management Risks**

Risks are assessed by identifying threats and vulnerabilities to the Medical Inventory Management System of George Washington Hospital, and then determining what the impact and likelihood of each risk are. Although assessment of the dangers is involved, it is evident that any malicious attacks to the system will impact the patients, nurses, personnel and the hospital as a business. Therefore, to minimize potential threats, hospitals must work with professional healthcare security and risk managers to assess, identify and evaluate risks or threats to the Medical Inventory Management System information assets. Potential risks will cause an undesirable outcome resulting in a negative result or consequences to the hospital's mission and objectives.

Step 7: Analyze Risks

- **Patient Health Records Analyze Risks**

The employees of GWU hospital should understand the risk and know the risk management plan in case of adverse events. The risk management strategy should also include the external attacks. The employees should know what to do, who to call, and how to decrease the possible negative impact and outcome.

- **Staff Analyze Risks**

Risk analysis is about developing an understanding of the risks identified. Staff should be aware of the level and importance of the risk. Also, a team should figure out the cause of the risk and how they can mitigate the risks in order not to have an impact in the long term.

- **Facility Analyze Risks**

Risk analysis includes identifying specific risks to each type of asset and determining its severity, probability of occurrence, and effectiveness of potential proactive and reactive measures. Risk analysis is a collaborative process requiring security experts to work in tandem with stakeholders so that every possible threat is identified and properly analyzed.

- **Network Analyze Risks**

When attackers attack GWU hospital's network, the GWU hospital's network can not work regularly. Patients and doctors cannot use network either. Doctors can't look at the patient's' records in their computers through connecting networks, and patients can't pay their medical charges online or in a hospital because GWU hospital needs the network to connect to the bank and verify their trades. Moreover, people can't go to the GWU hospital's website to look some information.

- **Online Transaction Data Analyze Risks**

Impact Value is a qualitative value assigned to describe what the impact GWU Hospital would get when a threat to Online Transaction Data is realized. Under the Risk Measurement Criteria, our team consider the context of GWU Hospital organizational drivers to generate a relative risk score for risk analysis and risk strategy implementation in the column (8) of Online Transaction Data Risk Worksheets. We assign impact values as follows: High – 3, Medium – 2, and Low – 1. We clarify that scores in Analyze Risks are only used as a prioritization tool. The risk with a higher score is relatively more important to GWU Hospital than the lower-score risk, and there is no importance to the different points.

- **Medical Inventory Information Analyze Risks**

Risk analysis is a complex undertaking which measures the extent to which a threat impacts George Washington Hospital. It can be performed by applying the knowledge of the organisation and some common sense. Risk analysis results indicate the direct effects on the hospital's reputation, potential monetary losses and lawsuits, and possible fines and penalties that the hospital should be aware of it. Once the consequences of a risk affecting the hospital as compared to the relative importance of the various impacted areas are known, its mitigation can be prioritized accordingly. Since the area of ‘modify patient medication' is the most important to George Washington Hospital and the consequences of the risk causes an extensive impact to the hospital, an immediate action must be taken to ensure the risk is mitigated.

Step 8: Select Mitigation Approach

- **Patient Health Records Mitigation Approach**

The risk the GWU hospital face for this specific asset is the loss or disclosure of the confidential health records. The best approach would mitigate the risk. The failure or exposure of the vital asset would cause the long-term impact on the GWU hospital. The residual risk of losing or disclosing data is the long-term impact the GWU hospital need to accept and continue decreasing the negative impact. The risk mitigation manual should be well-written and learned by every staff who have access to patient health records. The mitigation strategies should be simple and easy to start with. The employees need to know the signs of potential attacks and should keep in mind the possible disastrous outcome. In the training session, the management team should always stress the importance of the mitigation strategy and ask employees to follow.

- **Staff Mitigation Approach**

Some threats are challenging to be detected because of the nature of the problem, and we cannot just give blind trust to staff and employees. Because internal breaches are often carried out using normal modes of operation, we can't use traditional tools, like firewalls or antivirus software to stop and avoid them. Instead, we have to build a security strategy that can handle internally as well as external cybersecurity issues.

Self-policing of staff is an essential part of the threat strategy, but it is not the whole story. This risk can be mitigated by applying a few actions on technical and administrative containers. Technically, each staff should have the minimum required access to the system, but due to updates and changes to the system, it would be recommended to check the access for each role regularly. Another mitigation plan is a background check on staff and whoever has access to the system for preventing incidents. The risk can also be mitigated by regular training of staff and employees at the hospital.

- **Facility Mitigation Approach**

As described in previous sections, the information security management system must include plans and procedures to identify, prevent and mitigate the potential threats and security risks. The following section describes few examples are mitigation measures as applicable to GWU hospital:

1) Laboratory and test facility staff should be well trained on day-to-day security procedures and the process to follow in case of an incident. Supervisors are responsible for ensuring that new personnel are adequately trained and that training records of all staff are maintained on file.

2) Equipment must be positioned and secured correctly such that they are not exposed to imminent environmental threats, which includes potential exposure to hazardous material, direct natural light and water, as applicable to each equipment. Unauthorized access is another instance of potential security threat.

3) Interruption to equipment critical feeding sources such as power, gas, water, and communication as well as supporting utilities like drainage, sewage, and HVAC is another security risk that can impacts equipment functionality and can comprise security.

4) Unauthorized relocation of equipment, files, and other informational assets within and outside of secured site is another potential security risks that should be considered and mitigated.

- **Network Mitigation Approach**

The Center for Internet Security (CIS) offers twenty highly effective and widely accepted recommendations called the Critical Security Controls (CSC). These controls act in order of significance but often are not practical for businesses that may not have the required or necessary budget. The controls offer a top-down approach to a layered defence or defense-in-depth. As such, many of the controls overlap to some degree. By analyzing these overlapping controls, GWU hospital can create minimum baseline security postures, while saving the overhead costs. They can then implement the full powers over time. If budget and time constraints are a pressing issue, GWU hospital can narrow the scope of implementation for the authorities and focus on email and web-based attacks as these are the most common vectors used by attackers.

- **Online Transaction Data Mitigation Approach**

The mitigation approach for Online Transaction Data, consisting accept, mitigate and defer, is the way that how GWU Hospital addresses a risk. Accept means to take the consequences and not to address a risk. Mitigate means to discuss a threat that could have a medium to high impact on GWU Hospital's online transaction Data by developing and implementing controls by minimizing the resulting implication, or both. When a risk for GWU Hospital is neither accepted nor mitigated, the deferment will happen and risks deferred are not an imminent threat to the organization. All related further analysis would be found in the Worksheet (8).

- **Medical Inventory Information Mitigation Approach**

The risk is limited by implementing controls that minimize the adverse impact of a threat exploiting a vulnerability (3). George Washington University Hospital address risks based on their risk score. The mitigation approach assigned to each of the dangers is highly dependent on the hospital's circumstances. Since disruption of Medical Inventory Management System will have an imminent impact and result in hurting the hospital's reputation the most, this risk needs immediate mitigation. To minimize the threats, the best mitigation strategy is to apply multiple security countermeasures and a layered defensive strategy which includes patch management, configuration control, application whitelisting, memory protection, data encryption, port device control and firewalls and antiviruses. A defense-in-depth strategy minimizes the threats

Also, internal intentional hacks of the system threats can be mitigated by limiting users' unnecessary access to the system and also conduct the vigorous background check on the internal users to limit and minimize potential threats. The hospital should prioritize its risk mitigation activities based on the probability of threat and its impact.

Appendix

PART 1: Risk Measurement Criteria

Allegro Worksheet 1	Risk Measurement Criteria – Reputation		
Impact Area	**Low**	**Moderate**	**High**
Reputation (Staff)	**Reputation among non-physician hospital staff is minimally affected; little or no effort or expense is required to recover.**	**Reputation among non-physician hospital staff is damaged. No more than $100K in time and effort required recovering.**	**Reputation among non-physician hospital staff is severely damaged. More than $100K in time and effort required recovering. Relationship with faculty is affecting reputation with physicians and community. The poor relationship was affecting hospital efficiency and having the noticeable effect on bed turnover rate.**
Reputation (Physician))	**Reputation among physicians is minimally affected; little or no effort or expense is required to recover. Little or no change in hospital occupancy rate.**	**Reputation among physicians is damaged, causing physician population to reconsider sending patients to the hospital. Occupancy rate changes of between one and five percent directly attributable to reputation problem. More than $100K in time and effort required recovering.**	**Reputation among physicians is severely damaged. Critical staff physicians and hospital-affiliated physicians are considering leaving. Occupancy changes of more than five percent are directly attributable to reputation problems. More than $500K in time and effort required recovering.**
Reputation (Customers)	**Reputation in the community from which hospital draws patients is minimally affected; little or no effort or expense is required to recover. Little or no change in hospital occupancy rate.**	**Reputation in the community is damaged, causing potential patients to baulk at doctor recommendations to the hospital. Occupancy rate changes of between one and five percent directly attributable to reputation. More than $100K in time and effort required recovering.**	**Reputation in a community is severely damaged, causing potential patients to refuse doctor recommendations to the hospital. Occupancy rate changes of more than five percent are directly attributable to reputation problem. More than $500K in time and effort required recovering.**

Allegro Worksheet 2	**Risk Measurement Criteria – Financial**		
Impact Area	**Low**	**Moderate**	**High**
Operating Costs	**Increase of less than 2.61% in annual operating costs**	**Increase of between 2.61% and 7.3 % in annual operating costs**	**Increase of more than 7.3% in annual operating costs**
Revenue Loss	**Less than $150K reduction in yearly revenue loss**	**Between $150K and $1M in yearly revenue loss**	**More than $1M in yearly revenue loss**
One-Time Financial Loss	**Less than $100K reduction in yearly revenue loss**	**Between $100K and $1M in yearly revenue loss**	**More than $1M in yearly revenue loss**

Allegro Worksheet 3	**Risk Measurement Criteria – Productivity**		
Impact Area	**Low**	**Moderate**	**High**
Staff Hours	**Staff work hours increase labour costs by less than $150K.**	**Staff work hours increase labour costs between $150K and $1M.**	**Staff work hours increase labour costs by more than $1M.**
Other: Bed Turnover Rate	**The turnover rate for hospital beds decreases less than 2%.**	**The turnover rate for hospital beds decreases between 2% and 5%.**	**The turnover rate for hospital beds decreases by more than 5%.**

Allegro Worksheet 4	**Risk Measurement Criteria – Safety and Health**		
Impact Area	**Low**	**Moderate**	**High**
Life	**No significant threat to lives and no regulatory response.**	**Customers’ or staff members’ lives are threatened, but they will recover after receiving medical treatment. Only minimal regulatory response and less than $250K in related costs.**	**Loss of customers' or staff members' lives. The significant regulatory response, lawsuits, and more than $250K in related costs.**
Health	**Minimal, immediately treatable degradation in customers’ or staff members’ health with recovery within days. Minimal regulatory response and less than $100K in related costs.**	**Temporary or recoverable impairment of customers’ or staff members’ health. Only minimal regulatory response and between $250 and $500K in related recovery costs.**	**Permanent impairment of significant aspects of customers' or staff members' health. A significant regulatory response involving investigations and more than $500K in recovery costs.**
Safety	**Safety questioned, but no regulatory response and little to no economic cost.**	**Safety affected minimal regulatory response and less $250K in recovery costs.**	**Safety violated the significant regulatory response involving investigations and more than $250K in recovery and response costs.**

Allegro Worksheet 5	**Risk Measurement Criteria – *Investigations***		
Impact Area	**Low**	**Moderate**	**High**
Investigations	**No queries from the government or other investigative organizations.**	**Government or other investigative organization requests information or records (low profile).**	**Government or other investigative organization initiates a high-profile, in-depth investigation into organizational practices.**

Allegro Worksheet 6	Impact Area Prioritization Worksheet
Priority	**Impact Areas**
1	**Reputation**
2	**Financial**
3	**Productivity**
4	**Safety**
5	**Health**

PART 2: Critical Information Assets

Allegro Worksheet 7	**Critical Information Asset Profile**	
(1) Critical Asset ***What is the critical information asset?***	**(2) Rationale for Selection** ***Why is this information asset important to the organization?***	**(3) Description** ***What is the agreed-upon description of this information asset?***
Health Record System	**For the hospital, patients are the most important stakeholders. Their medical records and personal information are sensitive and crucial.**	**The patient information contains personal information such as name, address, and age. Another part is the medical record of an individual patient which contains specific details of him or her.**
(4) Owner(s) ***Who owns this information asset?***		
Patients		
(5) Security Requirements ***What are the security requirements for this information asset?***		
Confidentiality	**Only authorized personnel can view this information asset, as follows:**	**The GWU hospital is running under HIPAA privacy rule to protect patient records. Only authorized employees and patients themselves can have access to the data.**
Integrity	**Only authorized personnel can modify this information asset, as follows:**	**Authorized doctors, nurses, and employees can modify and make changes to patients' records.**
Availability	**This asset must be available for this personnel to do their jobs, as follows:**	**The system needs to be available for patient and doctors.**
	This asset must be available for 24 hours, seven days/week, and 54 weeks/year.	
	This asset has special regulatory compliance protection requirements, as follows:	**HIPAA Privacy Rule**

(6) Most Important Security Requirement
What is the most important security requirement for this information asset?

Confidentiality	**Integrity**	**Availability**	**Other**

Allegro Worksheet 8	**CRITICAL INFORMATION ASSET PROFILE - STAFF**	
(1) Critical Asset ***What is the critical information asset?***	**(2) Rationale for Selection** ***Why is this information asset important to the hospital?***	**(3) Description** ***What is the agreed-upon description of this information asset?***
Staff Information	**If it is disclosed, it hurts the effectiveness of the hospital and the.**	**Staff Information Database.It contains all personal, financial, and HR related information about the doctors, nurses, and employees of the hospital. This asset contains very sensitive information about all individuals working for the hospital: DOB, salary, performance, bank accounts, background information, SSN, medical records**
(4) Owner(s)		
Division of Human Resources and Benefits Administration		
(5) Security Requirements		
Confidentiality	**Only authorized personnel can view this information asset. Since staff information database may contain highly sensitive personal and financial information of employees, only the right to know HR personnel be allowed to access relevant part of the database.**	**The HR of the hospital should decide role-based access rights to the relevant part of staff information.** **The staff to access their portal should use Strong Authentication.**
Integrity	**Only authorized personnel can modify this information asset. Maintaining accurate records of staff data ensures that the intended data is the same as it was originally provided to HR and recorded in the database.**	**Inputs to staff information can be received from various sources, and maintaining data integrity is important to the generation of accurate, relevant reports.**
Availability	**This asset must be available for HR and directors to do their jobs.**	**Other than HR employees, employee information database may be accessed by hiring managers, payroll processes, and benefits administration for their day-to-day operations.**
	This asset must be available under strong authentication and privacy control.	

Other	This asset has special regulatory compliance protection requirements, as follows:		
(6) Most Important Security Requirement			
Confidentiality	Integrity	Availability	Other

Critical Assets -- Online Transaction

Allegro Worksheet 11	**Information Asset Profile**	
Critical Asset	**(2) Rationale for Selection**	**(3) Description**
Online Transaction Records	**An accurate online transaction record is essential for negotiating, billing customers and collecting compensation. Challenges mainly exist in bills from insurance organizations can express from billing differences, which may delay the time between services**	**This information asset contains all of the information necessary to bill a patient and insurance company for treatment or services received from the GWU Hospital.**
(4) Owner(s)		
The owner of this information asset is the Director of Patient Billing and Collection.		
(5) Security Requirements		
Confidentiality	**Only authorized personnel can view this information asset, as follows:**	**The access to data should be based on the role. Members of the hospital financial staff responsible for billing and collection. Other financial staff can have access to summary information. Data entry personnel should have "read" access to individual records.**
Integrity	**Only authorized personnel can modify this information asset, as follows:**	**Only authorized data entry personnel and members of the hospital financial staff may update/change billing record information.**
Availability	**This asset must be available for this personnel to do their jobs, as follows:**	**The Online Transaction data must be available to data entry personnel for updates to billing and procedures codes and for admitting purposes. The database was available to financial staff for billing and collection activities.**

(6) Most Important Security Requirement			
Confidentiality	Integrity	Availability	Other

PART 3: Assets Containers

Allegro Worksheet 9a	**Information Asset Risk Environment Map (Technical)**
Internal	
Container Description	**Owner(s)**
1. Billing Management System (BMS). The IT department oversees and manages the electronic health record system.	**GWU Hospital**
2. Hospital internal network. All transactions to and from the BCD system travel on this network.	**Managed by hospital IT department.**
3. Hospital workstations (e.g., order entry workstations, finance department workstations, and hospital admitting workstations).	**Managed by hospital IT department.**
4.The staff Information Database is used by the HR systems to record employment, benefits, deductions, and wage payment information.	**GWU Hospital**
5.Payroll process, HR reporting and analytics, benefits administration, employment eligibility process, and hiring doctors, nurses and staff are using this database.	**HR**
External	
Container Description	**Owner(s)**

1. The company who made the online health record system. The specific company has the responsibility to provide further technical services for GWU hospital if the internal (IT department of GWU hospital) cannot solve the problem.	**Company who made the online health record system**
GWU External Internet: Most bills are electronically emailed to insurance providers each week.	**Unknown**
Allegro Worksheet 9b	**Information Asset Risk Environment Map (Physical)**
Internal	
Container Description	**Owner(s)**
1. File Folders: Paper copies of billing summaries are printed and kept in file folders by the finance department.	**Financial Office of GWU Hospital**
2. Super Server: Paying an invoice requires information automated stored on the Super Server of GWU Hospital	**Managed by hospital IT department.**
3. Backup tapes: Backup tapes of BMS are created periodically and kept onsite until regular pickup by storage vendor.	**GWU IT department**
External	
Container Description	**Owner(s)**

1. File Folders: Paper copies of billing statements are regularly kept in File Folders	**Financial Office of GWU Hospital**
2. File Folders: Paper copies of billing statements, summaries, histories, and reports are regularly printed and mailed to insurance providers.	**Financial Office of GWU Hospital**

Allegro Worksheet 9c	Information Asset Risk Environment Map (People)
Internal Personnel	
Name or Role/Responsibility	Department or Unit
1. Admitting staff (John Jones)	Admissions
2. Order entry staff (Amy Green)	Business Services
3. Financial staff	Business Services
4. Hospital messenger service staff	Business Services
External Personnel	
Contractor, Vendor, Etc.	Organization
1. Insurance organization’s claims staff	Hospital Insurance, Inc.

2. Third-party vendor manages the transportation and storage of backup tapes for the BCD system. The relationship is managed via the hospital IT department.	**Data Storage, Inc.**

Allegro Worksheet 9b	**Information Asset Risk Environment Map (Physical)**
Internal	
Container Description	**Owner(s)**
1. **GWU Hospital provides physical storage for the critical health record system and patients information database.**	**GWU Hospital**
External	
Container Description	**Owner(s)**
1. **The company who made the system will provide external backup as part of technical support in case any emergencies occur.**	**Company who made the online health record system**

Allegro Worksheet 9c	**Information Asset Risk Environment Map (People)**
Internal Personnel	
Name or Role/Responsibility	**Department or Unit**
1. **GWU Hospital authorized employees can have access to the health record system. For instance: doctors, nurses, and authorized employees who can modify medical records.**	**GWU Hospital IT department**
	HR department
External Personnel	
Contractor, Vendor, Etc.	**Organization**
1. **The employees in the company who have access to the system and the sensitive medical records are the external personnel.**	**Company who made the online health record system**

Medical Inventory Information

Allegro Worksheet 9a	**Information Asset Risk Environment Map (Technical)**
Internal	
Container Description	**Owner(s)**
1. GWU Hospital IT Department. The IT department oversees and manage the medical inventory information.	**GWU Hospital**
External	
Container Description	**Owner(s)**
1. The vendor who made medical inventory management system. The vendor provides maintenance technical support.	**Medical Inventory Management System Vendor**

Allegro Worksheet 9b	**Information Asset Risk Environment Map (Physical)**
Internal	
Container Description	**Owner(s)**
1. GWU Hospital provides physical storage for the medical inventory management information and its database.	**GWU Hospital**
External	
Container Description	**Owner(s)**
1. The vendor company provides external backup of the data as part of their technical support in case of emergencies.	**The vendor who made the medical inventory management system.**

Allegro Worksheet 9c	Information Asset Risk Environment Map (People)
Internal Personnel	
Name or Role/Responsibility	Department or Unit
1. GWU Hospital authorized employees can access medical inventory information. For instance: pharmacists, doctors, nurses, accountants, and warehouse staff.	GWU Hospital IT department
	HR department
External Personnel	
Contractor, Vendor, Etc.	Organization
1. The vendor company employees who have access to the system and medical inventory data are the external personnel.	The vendor who made the medical inventory system.

Part 4 Risk Worksheet

Health Record System Concerns

Allegro - Worksheet 10			**Information Asset Risk Worksheet**	
Information Asset Risk	**Threat**	**Information Asset**	**Health Record System**	
		Area of Concern	**Data breach or potential hacking both internally and externally**	
		(1) Actor ***Who would exploit the area of concern or threat?***	**Internal employees or external hackers**	
		(2) Means ***How would the actor do it? What would they do?***	**For internal employees, they would pass security and stole sensitive data.** **For external hackers, they would hack the data. DOS may be a possible hacking method**	
		(3) Motive ***What is the actor's reason for doing it?***	**Financial reason**	
		(4) Outcome ***What would be the effect on the information asset?***	**Disclosure** **Modification**	**Destruction** **Interruption**
		(5) Security Requirements ***How would the information asset's security requirements be breached?***	**Once the hacker has access to the system, he/she can access the database and disclose patients' information.**	

(6) Probability ***What is the likelihood that this threat scenario could occur?***	**High**	**Medium**	**Low**
(7) Consequences ***What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?***	**(8) Severity** ***How severe are these consequences to the organization or asset owner by impact area?***		
	Impact Area	**Value**	**Score**
The outcome of this will be impacting the GWU hospital in long-term operations.	**Reputation & Customer Confidence**	High	12
	Financial	High	12
	Productivity	High	9
	Safety & Health	Low	5
	Fines & Legal Penalties	High	12
	User Defined Impact Area		
		Relative Risk Score	50

(9) Risk Mitigation ***Based on the total score for this risk, what action will you take?***			
Accept	**Defer**	**Mitigate**	**Transfer**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	***What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?***		
Firewalls	Find a trustworthy Firewall system that GWU hospital can use. Update the firewall regularly, which prevent the possible external attacks. The residual risk of losing the health records would be long-term reputation impact. Patients may choose other hospitals over GWU hospital because of this. How to rebuild the broken trust is the residual risk that GWU hospital needs to accept.		

Allegro Worksheet 8	Critical Information Asset Profile	
(1) Critical Asset	(2) Rationale for Selection	(3) Description
Network	There are many works on the GWU hospital based on the network. Patients can pay the fee for the hospital network, and doctors can see patient's digital records through the hospital network. And it is important to keep its security.	The network operator provides the network service to the GWU hospital and keeps its security before the data connect to the hospital.
(4) Owner(s)		
The owner of this information asset is the Director of Hospital Network Department.		
(5) Security Requirements		
Confidentiality	Only authorized personnel can view this information asset, as follows:	Doctors can connect the network through the hospital desk computer, which has been authorized by the MAC address.
Integrity	Only authorized personnel can modify this information asset, as follows:	The manager of the GWU hospital network department has access to modify the network in a hospital.
Availability	This asset must be available for this personnel to do their jobs, as follows:	Patients can connect the wireless network when they in GWU hospital and they need to be authorized.

(6) Most Important Security Requirement			
Confidentiality	**Integrity**	**Availability**	**Other**

Allegro Worksheet 9a	**Information Asset Risk Environment Map (Technical)**
Internal	
Container Description	**Owner(s)**
1. **The medical network service can replace or supplement some or all of an expensive internally staffed clinical facility network with a cloud-based networking service. And GWU hospital creates the wireless network in their offices and wards by many routers.**	**The department of GWU hospital network**
External	
Container Description	**Owner(s)**
1. **Network operator provides the network to GWU hospital and keeps it security and normal.**	**Network operator**

Allegro Worksheet 9b	**Information Asset Risk Environment Map (Physical)**
Internal	
Container Description	**Owner(s)**
1. **There are some network servers in the GWU network servers room and GWU hospital stores the network data and information in this room.**	**The department of GWU hospital network**
External	
Container Description	**Owner(s)**
1. **Network operator monitors the network data from the GWU hospital in operator's servers room.**	**Network operator**
Allegro Worksheet 9c	**Information Asset Risk Environment Map (People)**
Internal Personnel	
Name or Role/Responsibility	**Department or Unit**
1. **GWU Hospital authorized employees can have access to connect the hospital’s network and view the health record system.**	**The department of GWU hospital network**

External Personnel	
Contractor, Vendor, Etc.	**Organization**
1. **Patients in GWU hospital can connect wireless network and pay the fee by hospital's network.**	**The department of GWU hospital network**

Allegro - Worksheet 10			**Information Asset Risk Worksheet**		
Information Asset Risk	Threat	**Information Asset**	**Online Transaction Data**		
		Area of Concern	**Online Transaction Data is altered when unauthorized individual gains access to GWU Hospital BMS system.**		
		(1) Actor	**Disgruntled current employees**		
		(2) Means	**Using workstation on the internal hospital network, employee launches the attack on GWU Hospital BMS system.**		
		(3) Motive	**Wants to harm hospital because of ongoing labour contract disputes**		
		(4) Outcome	**Disclosure** **Modification**		
		(5) Security Requirements	**Only authorized members of the hospital data entry staff and finance staff should be able to modify BMS asset.**		
		(6) Probability	**High**	**Medium**	**Low**
	(7) Consequences		**(8) Severity**		
			Impact Area	**Value**	**Score**
	If insurance companies are not charged correctly for services, the hospital will lose money.		**Reputation**	**Low**	**2**
			Financial	**High**	**12**

	Charges need auditing.	Productivity	High	9
		Safety & Health	Low	5
	Exposure of patient data may lead to fines and possible lawsuits.	Investigation	Med	2
Relative Risk Score				**30**

(9) Risk Mitigation			
Accept	**Defer**	[✓ **Mitigate**]	**Transfer**
For the risks that you decide to mitigate, perform the following:			

On what container would you apply controls?	***What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?***
Hospital network	**Restrict network traffic to ensure correct BMS authorisation.**
BMS	**Auditing Transaction**
BMS	**Update BMS system**

Allegro - Worksheet 10			Information Asset Risk Worksheet		
Information Asset Risk	Threat	Information Asset	Online Transaction Data		
		Area of Concern	DoS attack against GWU Hospital network destroys the hospital's ability to electronically deliver bills to the insurance organizations.		
		(1) Actor	A hacker who wants to see if he can damage the hospital financially		
		(2) Means	Uses DoS toolkit found on a hacking website.		
		(3) Motive	Entertainment		
		(4) Outcome	Disclosure Modification	Destruction Interruption	
		(5) Security Requirements	The OTD must be available for billing and collection activities.		
		(6) Probability	High	Medium	Low
	(7) Consequences		(8) Severity		
			Impact Area	Value	Score
	GWU Hospital must burn CDROMs with the data. Significant financial impacts.		Reputation	Med	4
			Financial	High	12
			Productivity	High	9

		Safety & Health	Low	5
		Investigation	Low	1
Relative Risk Score				31

(9) Risk Mitigation

Accept	Defer	[✓ Mitigate]	Transfer

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Internet	Find a new service provider who has more robust connectivity solutions and can be more supportive in preventing DoS attacks.
Internet	Work with insurance companies to develop alternative delivery methods such as a direct connection.

Allegro Worksheet 10			**Information Asset Risk Worksheet**		
Information Asset Risk	**Threat**	**Information Asset**	**Online Transaction Data**		
		Area of Concern	**The workstation connected to BMS server in a public area is accessible by visitors.**		
		(1) Actor ***Who would exploit the weakness?***	**Hospital staff and/or inquisitive patients or hospital visitors**		
		(2) Means ***How would the actor do it? What would they do?***	**When no one is at the workstation, a hospital worker, patient, or visitor could access data.**		
		(3) Motive	**Curiosity**		
		(4) Outcome	**Disclosure** **Modification**	**Destruction** **Interruption**	
		(5) Security Requirements	**Only authorized personnel can view this information asset.**		
		(6) Probability	**High**	**Medium**	**Low**
	(7) Consequences		**(8) Severity**		
			Impact Area	**Value**	**Score**
	Exposure of patient sensitive information opens the hospital to lawsuits and fines for breaches of HIPAA regulations.		**Reputation & Customer Confidence**	**High**	**6**
			Financial	**Med**	**4**
	The public's overall perception of the hospital's quality could be negatively affected if the patient		**Productivity**	**Low**	**3**

	sensitive information is publicized.	Safety & Health	Low	5
		Fines & Legal Penalties	Med	2
Relative Risk Score				20

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

Accept	**Defer**	**[✓ Mitigate]**	**Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	***What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?***
Hospital workstations	**The screen is locked.**
BMS	**Enable transaction logging on the BMS system.**
BMS	**Least Privilege**
Admit staff	**Responsibility training.**
Data entry staff	**Responsibility training.** **Create non-disclosure Policies**
Financial staff	**Responsibility trainings.** **Create non-disclosure Policies**

Allegro Worksheet 10			**Information Asset Risk Worksheet**		
Information Asset Risk	**Threat**	**Information Asset**	**Online Transaction Data**		
		Area of Concern	**Staff leave paper copies of billing summaries on their desks.)**		
		(1) Actor ***Who would exploit the weakness?***	**Janitorial staff**		
		(2) Means ***How would the actor do it? What would they do?***	**Sees billing summary while cleaning an office**		
		(3) Motive ***What is the actor's reason for doing it?***	**Curiosity**		
		(4) Outcome ***What would be the effect on the information asset?***	**[✓ Disclosure]** **Modification**	**Destruction** **Interruption**	
		(5) Security Requirements ***How would the information asset's security requirements be breached?***	**Only authorized personnel can view this information asset.**		
		(6) Probability ***What is the likelihood that this threat scenario could occur?***	**High**	**Medium**	**Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	**Value**	**Score**
Exposure of patient sensitive information opens the hospital to lawsuits.	**Reputation & Customer Confidence**	**Med**	**4**
	Financial	**Low**	**4**
GWU Hospital’s quality could be negatively affected	**Productivity**	**Low**	**3**
	Safety & Health	**Low**	**5**
	Fines & Legal Penalties	**Med**	**2**
	User Defined Impact Area		
		Relative Risk Score	**18**

(9) Risk Mitigation *Based on the total score for this risk, what action will you take?*			
Accept	**Defer**	**Mitigate**	**Transfer**

For the risks that you decide to mitigate, perform the following:	
On what container would you apply controls?	***What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?***
Financial staff	▪ **Responsibility training for the financial staff.** ▪ **Online Transaction Data must be in locked cabinets.** ▪ **Paper copies are shredded at the end.** ▪ **Enact non-disclosure agreement.** ▪ **Perform regular audits.**
Janitorial staff	▪ **Enact a policy of non-disclosure agreements.**

Allegro Worksheet 10			Information Asset Risk Worksheet		
Information Asset Risk	Threat	Information Asset	Online Transaction Data		
		Area of Concern	Backup tapes break down.		
		(1) Actor *Who would exploit the weakness?*	Third-party backup storage provider		
		(2) Means *How would the actor do it? What would they do?*	Shipment of backup tapes is lost in storage.		
		(3) Motive *What is the actor's reason for doing it?*	Accidental		
		(4) Outcome *What would be the effect on the information asset?*	Disclosure Modification	[✓ Destruction] Interruption	
		(5) Security Requirements	Only authorized personnel can view this information asset.		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	High	Medium	Low
	(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*		(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
			Impact Area	Value	Score

	If backup tapes break down, all transaction will need to be restored.	**Reputation & Customer Confidence**	**Low**	**2**
		Financial	**High**	**12**
	There would be significant financial and productivity impacts to restore transaction.	**Productivity**	**High**	**9**
		Safety & Health	**Low**	**5**
	The restoration process charges incorrectly.	**Fines & Legal Penalties**	**Low**	**1**
		User Defined Impact Area		
			Relative Risk Score	**31**

(9) Risk Mitigation ***Based on the total score for this risk, what action will you take?***			
Accept	**Defer**	[✓ **Mitigate**]	**Transfer**
For the risks that you decide to mitigate, perform the following:			
On what container would you apply controls?	***What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?***		
Backup Tapes	**Keep a second copy of backup tapes on site.**		

Allegro Worksheet 10			**Information Asset Risk Worksheet**		
Information Asset Risk	**Threat**	**Information Asset**	**Online Transaction Data**		
		Area of Concern	**It seems that no one will check the data entry.**		
		(1) Actor ***Who would exploit the weakness?***	**Disgruntled data entry staff**		
		(2) Means ***How would the actor do it? What would they do?***	**Enters codes for test and procedures that were never performed**		
		(3) Motive ***What is the actor's reason for doing it?***	**Wants to harm the hospital**		
		(4) Outcome ***What would be the effect on the information asset?***	**Disclosure** [✓ **Modification**]	**Destruction** **Interruption**	
		(5) Security Requirements ***How would the information asset's security requirements be breached?***	**Billing records should only be updated with the actual billable services provided to the patient.**		
		(6) Probability ***What is the likelihood that this threat scenario could occur?***	**High**	**Mediu** **m**	**Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Impact Area	Value	Score
GWU Hospital might be sued for additional damages or negligence.	Reputation & Customer Confidence	Med	8
	Financial	High	12
The Auditing charges labour fees.	Productivity	High	9
	Safety & Health	Low	5
Insurance companies take too much time in reviewing, resulting in delays.	Fines & Legal Penalties	High	3
	User Defined Impact Area		
		Relative Risk Score	37

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

Accept	Defer	[✓ Mitigate]	Transfer

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	*What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?*
Data entry staff	▪ **Duties Separation.**
BMS	▪ **Enable transaction logging on the PBMS system.**
Financial staff	▪ **Billing Auditing periodically.**

Allegro - Worksheet 10			Information Asset Risk Worksheet		
Information Asset Risk	Threat	Information Asset	Hospital Network		
		Area of Concern	Attacked by hackers or malware		
		(1) Actor	Hackers who want the patient's record		
		(2) Means	They can attack the hospital’s network by DDOS or virus.		
		(3) Motive	They can sell the patient’s record and information to get money.		
		(4) Outcome	Disclosure Modification	Destruction Interruption	
		(5) Security Requirements	They can attack the hospital's network by DDOS or virus. And the hackers can make the backdoor when they break the hospital's network defence.		
		(6) Probability	High	Medium	Low
	(7) Consequences		(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
			Impact Area	Value	Score
	It will impact GWU hospital and their patient’s information.		Reputation & Customer Confidence	15	12
			Financial	15	10
			Productivity	15	12

		Safety & Health	**15**	**10**
		Fines & Legal Penalties	**20**	**18**
		User Defined Impact Area	**20**	**17**
Relative Risk Score				**79**

(9) Risk Mitigation

Based on the total score for this risk, what action will you take?

Accept	**Defer**	[✓ **Mitigate**]	**Transfer**

For the risks that you decide to mitigate, perform the following:

On what container would you apply controls?	***What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?***
GWU hospital network servers' room	**We can update the physical firewalls in network gateway and router and choose a high-level security firewalls for a system.**

Allegro Worksheet 11	Critical Information Asset Profile	
(1) Critical Asset	(2) Rationale for Selection	(3) Description
Online Transaction Data	An accurate online transaction record is essential for negotiating, billing, and paying payroll. Challenges exist in delays in insurance companies' billing difference.	OTD contains all of the information necessary to bill a patient and insurance company for the GWU Hospital.
(4) Owner(s)		
The owner of this information asset is the Director of Patient Billing and Collection.		
(5) Security Requirements		
Confidentiality	Only authorized personnel can view OTD.	Role-based access is necessary. For example, the financial staff is responsible for billing and collection. Data entry staff should have "read" access to online transaction records
Integrity	Only authorized personnel can modify this Online Transaction Data.	Only authorized data entry personnel have access to may update OTD
Availability	OTD must be available for specific persons.	The Online Transaction Data must be available to data entry personnel for updates to billing and procedures codes and for admitting purposes.
(6) Most Important Security Requirement		

Confidentiality	**Integrity**	Availability	Other

References

1. "The George Washington University Hospital Washington, DC". *Health Care Design Magazine*. Health Care Design Magazine.
2. https://www.gwhospital.com/sites/gwhospital.com/files/atoms/files/GW_Capabilities%20Brochure.pdf)
3. https://www.ncbi.nlm.nih.gov/books/NBK55881/
4. **https://www.gwhospital.com/patients-visitors/health-records-online**
5. **https://privacyruleandresearch.nih.gov/patients.asp**)
6. McClure, S., Scambray, J., Kurtz, G., & Kurtz. (2009). Hacking Exposed: network security secrets and solutions.
7. https://www.gwhospital.com/patients-visitors/health-records-online
8. *The George Washington University Hospital Defining Medicine*. (n.d.).
9. Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). *The OCTAVE Allegro Guidebook, v1.0*.
10. https://www.gwhospital.com/patients-visitors/health-records-online
11. https://privacyruleandresearch.nih.gov/patients.asp
12. https://www.ncbi.nlm.nih.gov/books/NBK55881/
13. https://resources.sei.cmu.edu/asset_files/TechnicalNote/2005_004_001_14507.pdf
14. http://blogs.harvard.edu/cybersecurity/files/2017/01/risks-and-threats-healthcare-strategic-report.pdf
15. http://resources.infosecinstitute.com/insider-threats-at-hospitals/#gref
16. Richard Hummel, (2017). Securing Against the Most Common Vectors of Cyber Attacks. (p.4)
17. http://elearning.scranton.edu/resource/business-leadership/purpose-of-risk-management-in-healthcare
18. https://www.elynsgroup.com/journal/article/steps-in-the-process-of-risk-management-in-healthcare