INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

CYBER-SECURITY THREAT:

BENCHMARKING CYBERSECURITY RESPONSE

PROCEDURE FOR HOSPITALS IN TEXAS

Institute for Homeland Security

Sam Houston State University

Narasimha Shashidhar

Cihan Varol

Khushi Gupta

Cyber-Security Threat: Benchmarking Cybersecurity Response Procedure for Hospitals in Texas

PI, and Co-PI: Cihan Varol and Narasimha Shashidhar

Doctoral Student Investigator: Khushi Gupta

Department of Computer Science
Sam Houston State University
Huntsville, TX
cxv007@shsu.edu, nks001@shsu.edu, kxg095@shsu.edu

Contents

The Benchmarking Documentation at a Glance

Figure 1 reflects the benchmarking documentation on cybersecurity procedures in Texas Hospitals. The rest of the document will cover each of the boxes in detail.

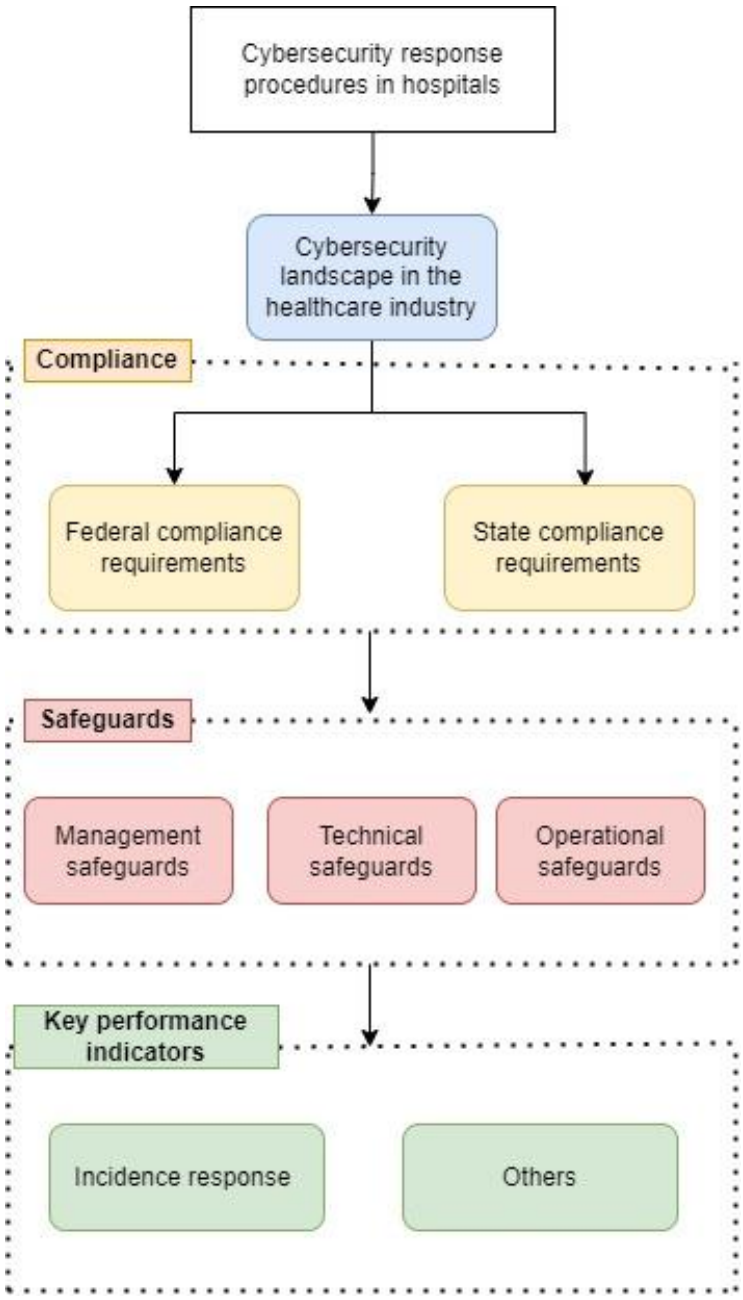


Figure 1: Benchmarking Document at a Glance

Introduction and Overview

A. Overview of the healthcare cybersecurity landscape (Types of attacks in hospitals)

Cyberattacks in the medical sector in Texas have spiked, threatening the operations of the systems and medical data. Hospitals are at a huge risk of cyberattacks moving forward. Here are some of the reasons why cyberattacks are seen at hospitals:

I. **Patient data is lucrative to attackers**: Medical facilities store an incredible amount of confidential patient information. This data is worth a lot of money when sold, making healthcare organizations a prime target.

II. **Medical devices provide an easy point of entry for attackers**: There are many medical devices such as insulin pumps, x-ray machines, defibrillators and many others that play a key role in the operations of modern healthcare systems. These devices are not designed with an information security mindset, instead they focus largely on the functionality of the device. While these devices may or may not store confidential medical information, they can open up more entry points for hackers to compromise the IT infrastructure of the organization.

III. **Increasing trends of remote collaboration and Telehealth services**: The healthcare industry is in a digital transformation phase. There has been an exponential growth in remote collaboration and telehealth services since the pandemic. While this shift opens doors to provide medical services remotely, it also comes with a risk that a hacker can also gain access to key information in the same manner.

IV. **Using outdated technology and legacy systems**: Outdated technology and legacy systems are still in use in the medical sector. These solutions were designed way before the healthcare industry was surrounded by cyber-attacks. Many older systems that are in operation today use insecure software leaving organizations vulnerable to cyberattacks.

V. **Lack of education and user training on online risks:** It is recommended that healthcare organizations invest in a dedicated cybersecurity team equipped with latest technology to fight against cyberthreats but, many attacks start as simple as getting key pieces of information from the staff. The lack of cybersecurity user training among medical staff can invite attacks such as impersonation, phishing, and social engineering tactics. This is usually the first step towards massive cybersecurity breaches in the medical industry.

Gap Assessment/ Problem statement

Several cybersecurity-related problems afflict the healthcare sector. These problems range from distributed denial of service (DDoS) assaults that impair hospitals' ability to deliver patient care to malware that compromises the security of systems and the privacy of patients. Cyber-attacks can affect the healthcare

industry in ways that go beyond monetary loss and privacy violations. Some of the most common cyberattacks faced by healthcare institutions are as follows:

1) **Ransomware attacks:** For hospitals, ransomware is a particularly heinous type of malware since the loss of patient data can put lives in danger. Once ransomware infects the system, it encrypts the files, and renders them inaccessible until the ransom is paid. These kinds of attacks are extremely dangerous as they can halt day-to-day operations by blocking access to data and systems.
2) **Malicious Network Traffic:** Malicious network traffic such as Distributed denial of service (DDoS) attacks is a common technique used to overwhelm the network and the system to a point of inoperability. This can prove to be a serious challenge to healthcare organizations as medical professionals will be unable to access the system to retrieve crucial patient information such as prescriptions or medical records.
3) **Phishing scams:** Phishing is one of the most popular first stages of a cyberattack. During a phishing scam, a person will be presented with a legitimate looking website. Upon interacting with it, it might ask for personal information or it might initiate malware which will then spread to other connected devices.
4) **Data breaches:** Data breaches refer to unauthorized data transfers. The number of healthcare institutions affected by data breaches has exponentially increased in number. Data breaches are widely observed in the medical sector in Texas. The types of data targeted include medical histories, insurance information, mental health conditions, laboratory results, social security numbers and so on. Since Personal Health Information (PHI) can become more valuable than Personally Identifiable information (PII), gaining access to medical information has become very lucrative to cybercriminals.

Topic Discussion

A. Regulatory and compliance requirements

Federal requirements

Before HIPAA, the healthcare sector lacked any generally recognized set of security standards or fundamental guidelines for safeguarding patient data. At the same time, as new technologies developed, the healthcare sector started to rely more and more on electronic information systems to handle a variety of administrative and clinical tasks. While this enables more flexible and effective medical personnel, the increased adoption of these technologies also raises the possibility of security risks.

HIPAA – The Health Insurance Portability and Accountability Act was established in 1996. It is a federal law that requires that the secretary of the U.S. Department of Health and Human Services (HHS) should develop rules to protect the privacy and security of certain health information. To that extent, HIPAA published the HIPAA privacy rule and the HIPAA security rule.

HIPAA security rule: This rule establishes a set of national security standards to protect health information that is stored or transferred in electronic forms. It operationalizes the technical and non-technical safeguards that organizations have known as "covered entities" must put in place to safeguard individuals' "electronic protected health information" (e-PHI) [1]. One of the major aims of this rule is to safeguard medical

information while also allowing covered entities to adopt new technologies so as to improve the efficiency and quality of healthcare they offer.

HITECH Act: The Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted as part of the American Recovery and Reinvestment Act of 2009. It was signed as a law on February 17, 2009, to promote the adoption of health information technology [2]. One of the goals of the act as covered by subtitle D is the privacy and security of electronic transmission of health data. This is enacted by provisions that strengthen the civil and criminal enforcement of HIPAA rules.

- **Tougher and stricter penalties for HIPAA violations:** Prior to the HITECH Act, the Office of Health and Human Services' (HHS) Office of Civil Rights could impose a maximum fine of $25,000. However, with HITECH, the fines were split into different tiers based on different levels of violations with a maximum financial penalty of around $2 million per category of violation per year as of 2022 (adjusted according to inflation).

- **HIPAA breach notification rule:** Under the new breach notification rule, covered entities are mandated to issue notifications to affected individuals within sixty days of discovery of a breach of unsecured protected health information [3]. The notification letter should include information such as:
    - Sent via first class mail.
    - The nature of the breach.
    - The types of protected health information are compromised.
    - Steps were taken to address the breach.
    - Actions that can be taken by affected individuals to reduce the potential of harm.

Additionally, breaches including records more than 500 in number should be reported to the HHS within 60 days of discovery. For smaller breaches, the notification should be sent within 60 days of the end of the calendar year in which the breach had taken place.

- **Access to Electronic Health Records:** HITECH changed the HIPAA right of access to personal health records so that individuals can obtain their health data in an electronic format so that it was easier to share their health data.

Healthcare Cybersecurity Act of 2022: Under this act, the Department of Health and Human Services (HHS) is mandated to take actions to improve the cybersecurity of the healthcare sector by coordinating with the Cybersecurity and Infrastructure Security Agency (CISA). Additionally, HHS must provide cybersecurity training in the medical sector [4].

Section 3305 of Consolidated Appropriations Act 2023 (Omnibus): This law amended the Federal Food, Drug and Cosmetic Act (FD&C Act) by adding section 524B called "Ensuring Cybersecurity of Devices". This bill establishes minimum cybersecurity standards for internet connected medical devices. This will ensure that healthcare devices are brought into the market with minimum certain standards developed by Food and Drug Administration (FDA) [5].

Federal Trade Commission (FTC) - Health Breach Notification (PHR, HER Vendors) 16 CFR Part 318: This regulation requires vendors of health records and related entities to notify consumers after a breach of information. If the breach involves more than 500 records, entities are required to notify the media.

Protecting and Transforming Cyber Health Care Act (PATCH) S.3983 – This law that was recently introduced in the Senate focuses on new requirements for medical devices and network security. This bill proposes the implementation of cybersecurity requirements for medical device manufacturers by requiring premarket approval from the FDA. Specifically, it will require the development of plans to identify and address post-market cybersecurity vulnerabilities and enable manufacturers to update and patch the systems throughout the device lifecycle.

State Requirements

Texas Medical Privacy Act: This act adopts HIPAA and expands the protections mandated by it. It provides extended patient privacy in three areas: a) it applies to a broader range of entities, b) it does not allow medical data to be marketed without patient authorization and c) prohibits the reidentification of information that has been de-identified [6].

Way forward

A. Incidence Response procedure benchmarking

This section includes benchmarks and guidelines for the key phases of the incidence response lifecycle for cyber-attacked Texas hospitals.

Preparation: This phase involves setting up and training an incidence response team while acquiring the essential tools and resources. In this phase, the organization also implements a series of controls to minimize the risk of cyberattacks.

Detection and Analysis: Despite the implemented controls, residual risk will persist. Thus, the detection of attacks and security breaches is key to alert the organization. This phase involves establishing procedures for the detection of attacks, escalating, and alerting the necessary personnel and prioritization, and analysis of the incident.

Containment, Eradication, and Recovery: Before the cyber-attack can extend its impact, the organization needs to implement measures to contain and ultimately recover from it. This phase involves the Cyber incidence response team conducting initial containment procedures, documenting the incident, and gathering evidence. The threat is then eradicated by shielding any vulnerabilities. Lastly, the systems are restored to full operation.

Post-incident activity: After the incident is adequately handled the organization should issue a report or take required steps such as a hot wash that describes the details of the root cause of the incident and future steps to prevent such incidents.

Management safeguards

Inventory systems and their data	• Identify critical business functions and the associated systems and data. • Identify people that support these critical functions. • Identify critical and sensitive data and the systems in which they reside. • Document and maintain a network architecture diagram.

Security and vulnerability assessments	• Adopt the HIPAA framework. • Constant check for advisories from vendors, virus alerts, US-CERT, etc. • Regularly schedule and conduct a thorough cybersecurity risk assessment to measure the current state, identify vulnerabilities and assess gaps (Penetration testing). • Share the assessment results with key stakeholders (senior leadership, CIRT team). • Determine the likelihood and impact of the identified vulnerabilities. • Determine the risk ratings of the relevant threats and vulnerabilities. • Analyze the current safeguards and their effectiveness to the identified risks.
Risk management program	• Implement a risk management program that clearly defines organizational risk appetite and tolerance, personnel duties, frequency of vulnerability and risk assessment, and required documentation. • Conduct risk assessment frequently while reevaluating past decisions, impact levels, and assessing effectiveness of past remediation efforts. • Ensure that remediation efforts reduce the risks and vulnerabilities to a benchmark level as stated in §164.306(a). • Develop a roadmap to address the gaps surfaced by the assessments based on the risk ratings.
Policies and procedures	• Create and document policies to accomplish security related tasks. • Establish a mechanism to communicate these policies to employees. • Create policies and establish roles for personnel to assign responsibility for the implementation of the controls related to the policy. • Establish a frequency to review policies and procedures.
Security policies	• Create and regularly update security policies. • Regularly update the processes and procedures used to protect critical systems.
Develop disciplinary policies	• Disciplinary policies should be developed for inappropriate access, use, and disclosure of confidential medical data. • Apply appropriate disciplinary actions against employees for noncompliance with the security policies in place. • Develop a formal process to implement the disciplinary policy when the need arises. • Make employees aware of the policy and the consequences. • Maintain a chain of notification for when the policies have been breached so that appropriate actions can be taken within time.
3rd party vendors	• Review current third-party tools, configurations, and the level of support provided by each vendor. • Maintain a list of service providers and evaluate the contracts for security considerations.
Security reminders	• Implement a method to regularly disseminate security-related updates such as newsletters, emails, messages, etc. to staff, business associates, partners, and contractors. • Implement security refresher training that is performed periodically. • Ensure the security awareness training is regularly modified and updated.
Vulnerability management process	• Implement a risk-based vulnerability remediation strategy. • Develop a plan of action and implement compensating controls for vulnerabilities found. • Implement a risk-based patch policy.

	• Test patches before deployment. • Enable automatic updates to operating systems and applications where applicable.
Identify all ePHI and the associated systems	• Determine the sources, entry points, movement, storage, and exit points of electronic protected health information (ePHI) within the organization. • Identify all systems, including mobile devices and medical equipment that handle ePHI, and all hardware (removable media) and software involved in the collection, storage, processing, or transmission of ePHI. • Analyze business functions and confirm ownership and control of information system components. • Document the current configuration of organizational systems to trace the flow of information and connections to other systems.
Acquiring IT systems and services	• Before procuring IT equipment, considerations should be taken into account on the security requirements of the organizations and the security features it provides.
Security organizational structure	• Document security assignments to the respective personnel and their job responsibilities/description. • Communicate these roles and responsibilities to the entire organization to create an easy notification chain in case of security events. • Ensure there is a chain of command throughout the structure. • Ensure there are open communication channels with senior officials in the organization such as CIO, CCO, executives, etc. • Establish lines of authority and appropriate levels of security oversight and access. • Document the different roles and the permission to view, alter, retrieve, and store ePHI at what times, what circumstances, and for what reasons.

Operational safeguards

Password Policy	**Proactive** • Implement a password policy (changing passwords regularly and selecting a password of appropriate strength). • Enable multi-factor authentication, especially for critical systems such as servers, administrative accounts, and remotely accessible accounts. • Disable default accounts and their credentials on assets such as medical devices. • Incorporate screen locks. **Reactive** • Change passwords regularly. • Have a mechanism for checking for leaked passwords.
Regular backup procedures	• Create a schedule to perform regular backups with priority given to critical systems and data. • Store the backups created online and if possible offsite. • Implement risk-based protections such as storing the backups in a fireproof location. • Test backups regularly. • Ensure the backups follow data management and protection rules (what data to retain and how long to retain it for).

	• Safeguard and securely store the backups (encryption and MFA to access the backups).

Security awareness training	• Ensure security awareness training is regularly provided to all users (including administrative staff, managers, and senior executives).
	• It should incorporate pointers from Texas Government code 2054.519(b).
	• Provide role-based training to security personnel.
	• Conduct training on risks identified during the risk assessment.
	• Ensure employees have a copy of the organization's security policy and procedures.
	• Ensure employees understand whom to contact and how to handle a security incident.
	• Some training pointers should include:
	  o Detecting and guarding against malware.
	  o Safeguarding passwords.

Assessing the training needs	• Itemize the training and education needed. • Monitoring current threats to determine new training areas. • Check if there are other medical IoT devices that the staff needs training on. • Implement a procedure to check if everyone in the organization has received and completed the required security training for their role. • Implement policies that sanction employees who have not completed the required training.
Personnel security requirements	• Ensure that employees and contractors are screened (background check) as required. • Incorporate escalating levels of scrutiny based on roles and data they have access to.
Develop incident response plan	• Establish and maintain an incident response plan to respond to incidents. • Test, conduct exercises on, and update the plan periodically. • Ensure the incidence response procedure encompasses all parts of the organization in which ePHI is created, stored, analyzed, and transmitted. • Determine the procedure for responding to a cyber incident. • Create a reporting mechanism for security incidents. • Determine the key functions of the organization that would be prioritized for restoration in case of an incident. • Have an incident response template to report pertinent information related to the incident. • Maintain a list of contacts that need to be contacted in case of a security breach. • Identify personnel that would communicate with external stakeholders (media, government agencies, etc.) in case of an attack.
Post incident considerations	• Analyze the incident (log files) to understand the nature and extent of the attack. • Keep a record of the incident and its outcomes. • Conduct an action review plan with relevant stakeholders. • After incident recovery, perform a security assessment to verify recovery activities. • Perform a gap analysis. • Perform a penetration test to verify recovery configurations. • Update and improve the security incident response procedures from the lesson learned in the breach.
Incidence response team	• Create an incident response team and maintain a stakeholder contact list. • Regularly train staff on the incident response plan.

	• Develop and maintain incident response procedures that act as a single point of reference for the day-to-day operations of the incident response team.
Contingency planning	• Draft a formal contingency plan that addresses pointers on disaster recovery data backup and identify preventative measures for scenarios that could result in loss of ePHI. • Define and establish an organizational chart, roles, and responsibilities for this area and train the personnel in those responsibilities. • Determine critical services that must be always provided e.g., patient treatment. • Identify software, hardware, and personnel critical to daily operations. • Identify cross functional dependencies to understand how failure in one system can disrupt other systems and services. • Determine the tolerance level and impact of unavailability of services. • Evaluate contingency measures (backups and redundancy). • Identify critical external service providers (cloud services, internet service providers, etc.) and ensure the reliability of their services via service level agreements. • Identify what data needs to be restored during an incident and what procedures will be taken to restore it. • Regularly test the contingency plan via tabletop exercises, document the test and revise the plan.
Physical security	• Inventory all the physical components in an organization and identify any vulnerabilities associated with them. • Establish the degree of significance for each vulnerability. • Establish policies for the usage of and safeguarding of physical assets such as data centers, equipment, and facilities. • Identify personnel responsible for the security of physical components. • Establish policies for the upgrade, repair, and modifications to physical components. • Implement access control procedures to validate that the person is allowed to access the equipment based on their role. • Document all the repairs, modifications, and access to the physical components of the organization.

Workstation security	• Inventory workstations and all other physical computing devices that store, transmit, create, and modify ePHI (medical equipment, IoT devices, tablets, and smartphones).
	• Classify physical computing devices by their functions, and mode of usage (onsite, remote, type of data handled).
	• Identify key operational risks that could jeopardize the security of the devices.
	• Develop policies for the prevention of the access of unauthorized users.
	• Employ safeguards for computing devices:
	  ○ Limiting device capabilities to access ePHI
	  ○ Limiting user permissions to access ePHI
	  ○ Device encryption
	  ○ Stringent access controls (e.g., multi-factor authentication)
	  ○ Screen lock
	  ○ Device management (e.g., Mobile Device Management [MDM], Endpoint Detection and Response [EDR])
	• Workforce education and training related to mobile and remote computing risks to ePHI.

Electronic media security	• Develop policies for the disposal of electronic media which stores ePHI such that previously stored data cannot be recreated. • Develop a process for the removal of ePHI before reusing the media again.

	• Maintain a record of the movements of physical devices (enterprise inventory management system). • Train employees on the security risks of reusing hardware. • Develop a procedure to extract a copy of the media and to check the integrity of the copy for forensic investigations or data backups. • Assign a unique identifier to electronic media for easy tracking.
Workforce clearance	• Conduct screening/background checks of personnel with access to ePHI.
Workforce termination policies	• Implement procedures to terminate access to ePHI when employment comes to an end (ID badges, keys, access cards, credentials). • Deactivate computer access accounts. • Establish a checklist of action items to be completed when an employee leaves. • Establish a clear communication process of informing third-party services of deactivation of accounts if necessary.

Technical safeguards

Access controls and account management policy	• Implement an automated procedure for requesting, creating, issuing, modifying, and deleting user accounts. • Determine the policies/conditions to create, modify, and delete user accounts. • Determine the policies for granting and restricting access to ePHI. • Assign privileges to user accounts on a need basis. • Actively monitor privileged accounts. • Implement multi-factor authentication. • Decided on what kinds of access control methods be put in place (identity-based, role-based, location-based, time-based, or more than one). • Regularly review access to ePHI to ensure the need for access and modifications.
Information assurance	• Set organization standards/expectations for the protection of ePHI. • Restrict the applications that can be run by end users to only supported software for official use. • Encrypt data in rest and transit. • Consider blocking unnecessary file types and features such as macros.
Cyber protection systems	• Implement and configure network defense tools such as firewalls (physical and virtual), antivirus software, and honeypots if necessary for servers and endpoints. • Keep systems up to date with the latest software versions and patches. • Implement a DNS filtering service. • Implement network-based filtering based on categories or reputation. • Securely administer remote software and hardware systems. • Implement segmentation in the network and filter malicious traffic between segments. • Implement email authentication services.
Malware protection	• Configure malware protection on computing devices. • Schedule periodic scans. • Disable auto-execute functions for removable media. • Configure group policies. • Incorporate Endpoint detection and response (EDR) systems.

Establish a log retention and review procedures	• Implement logging on critical systems. • Standardize logging stamps on all the logs. • Determine where and how long to retain system logs. • Implement procedures to regularly review logs of information system activity. • Establish the types of logs that will be reviewed and the corresponding personnel.
Technical safeguards for access control	• Consider segmenting the network to limit access to ePHI. • Implement procedures that terminate access to a session after a certain period of inactivity (screen lock). • Ensure access is always given following the least privilege principle. • Assign a unique identifier for each user so that their actions can be traced back to them. • Implement technical access control methods in accordance with the information access management policies. • Establish procedures for access control during initial access, increased access, access to different systems, and modification of access (if possible, automate these procedures). • Establish procedures for granting appropriate access during emergency situations. • Establish procedures to grant and revoke permissions and access for new employees and terminated employees (when and who will conduct the procedures.
Audit controls	• Develop policies on the intervals of auditing, analysis of logs, personnel involved, and consequences for employee violations. • Determine a safe location for audit logs to be stored. • From the risk assessment results, determine what activities need to be logged/audited. • Determine the data that needs to be logged (timestamps, users, event type, etc.). • Select the appropriate monitoring tools for the organization. • Develop a procedure to inform and communicate with managers and employees when suspicious activity is found.

Authentication	• Identify points of electronic access that require authentication.
	• Ensure the appropriate level authentication mechanisms are deployed for each access.
	• Use a combination of two or more of these authentication approaches:
	  ○ Something a person knows, such as a password.
	  ○ Something a person has or is in possession of, such as a token (e.g., smart card, hardware token, etc.).
	  ○ Some types of biometric identification.
	• Implement multi-factor authentication for better security.
	• Implement authentication mechanisms based on the results of the risk assessment.
	• Establish formal authentication policies and procedures and regularly maintain and update them.
	• Regularly test the authentication mechanisms to ensure they are working as needed.

Securing data in transit	• Identify all the routes through which ePHI will be transmitted in and out of the organization. • Identify scenarios that may result in the access and modification of the ePHI by unauthorized users during transmission. • Implement policies (transmission security policy) that detail the requirements for the transmission of ePHI. • Encrypt all the data in transit (email encryption and automated confidentiality statements.

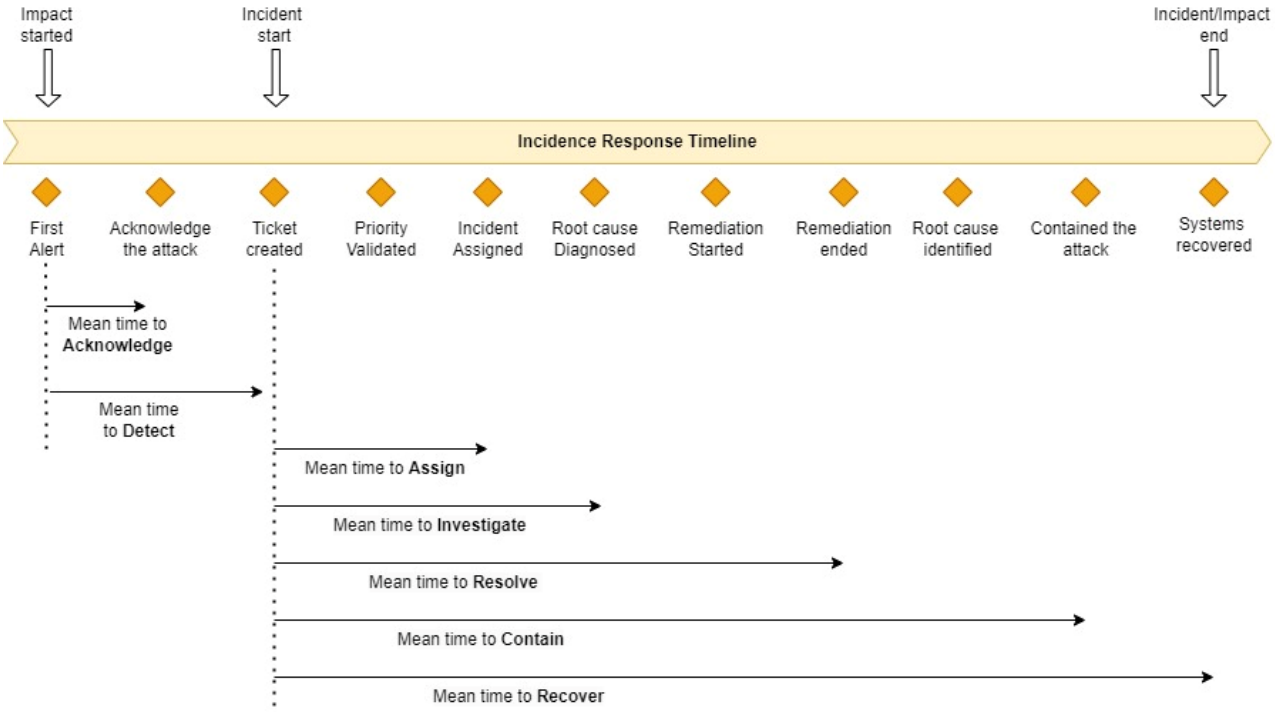
Integrity	• Identify sources that may result in the modification of data (insider theft, ransomware, hackers).
	• Establish policies on the integrity requirements of the data.
	• Implement technical solutions for the prevention and detection of malicious alteration and destruction of data (anti-malware, ant-ransomware, file integrity checking solutions).
	• Implement procedures that will protect ePHI from unauthorized modification and verify integrity:
	  ○ Digital signatures
	  ○ Error-correcting memory

B. Key Performance Indicators (KPI)

Incidence Response Timeline

KPI	Description	Assessment
Alerts created	Number of alerts created in a given period of time. (The number of false positive alerts created)	The higher the number of true positive alerts the more informed and comprehensive the better the incidence response posture is. **Number of alerts per day**
Mean time to acknowledgement (MTTA)	The average time it takes to acknowledge the existence of an alert which could be an outcome of an attack or security incident.	A lower MTTA indicates a more prompt and effective incident response process, enabling organizations to detect and address security incidents in a timely manner, thereby minimizing their impact and reducing the time for potential threats to persist undetected. **Minutes, Hours, Days**
Mean Time to detection	The average time it takes to notice a suspicious behavior that could be linked to an attack or incident	The lower the time, the better the incidence response program is. **Minutes, Hours, Days, Months**
Mean time to assign (MTTAs)	The average time it takes for an incident to be assigned to a responsible party or team for further investigation	A lower MTTAs indicates a more streamlined and effective incident response process. **Minutes, Hours, Days, Months**
Mean time to investigate an incident	The average time it takes to investigate an alert related to an incident	This metric will show how quickly the team is able to investigate an incident. **Minutes, Hours, Days, Months**
Mean time to resolve and contain an incident	The average time it takes to resolve and contain the attack.	The lower this metric is the stronger the incident response posture is. **Minutes, Hours, Days, Months**

	(Eradicate the threat, and prevent the threat actors from moving further into the system and network)	
Mean time to recover from an incident	The average time it takes to go from resolving and containing the attack to recovering from the attack and bringing the affected systems back to the pre-incident state.	The lower the metric, the more responsive the incidence response framework is. **Minutes, Hours, Days, Months**
Average Incidence Response Time	The average time it takes from the detection to the recovery of a security incident.	The less time it takes to go through the whole incidence response timeline the more responsive the incidence response program is. **Minutes, Hours, Days, Months, Years**



Other Key Performance Indicators

KPI	Description	Assessment
Patient Data Breach Rate:	The number of incidents involving unauthorized access, disclosure, or compromise of patient data.	The less patient data breach rate, the more effective the security controls and protection of confidential data. **Number of incidents per month/year**

Patient Data Recovery Time:	How much time does it take to recover sensitive data for normal operations to resume/?	The faster the rate of recovering patient data and other crucial information for normal operations, the more effective the incidence response program is. **Minutes, Hours, Days, Months, Years**
Clinical system downtime:	The time the medical systems experience downtime due to a security incident.	The less time the systems experience downtime, the less disruption it causes. **Minutes, Hours, Days, Months**
Medical device security incidents:	How many security incidents are traced back to medical devices?	The fewer security incidents that are traced back to the medical devices, the more secure the devices are. **Number of incidents**
Incident response team activation time:	The average time it takes from detecting an incident to assigning the incident and activating the incident response time.	The quicker the assignment and activation of the incidence response team, the quicker and more responsively the incident can be resolved. **Minutes, Hours, Days**
Incident backlog	Security incidents that are pending a resolution	The more pending security events, the less effective the incident response program is. **Number of pending incidents**
Compliance with data protection regulations:	The percentage of compliance of the security posture of the company with regulations.	The more the organization has complied with regulatory bodies, the better defense they have against security attacks and the better prepared they are to handle security incidents. **Percentage compliance with HIPAA, legal bodies, and rules**
Stakeholder (Patient, users, 3rd parties) notification and communication	The time taken to notify the affected users during a security breach/incident.	The faster the notifications are sent, the better the timeliness and effectiveness of the communication of the impact, risk, and mitigation measures. **Minutes, Hours, Days**
Incidence response training and awareness	The level of training and awareness among staff regarding incidence response procedures.	The more staff are trained in security procedures and concepts the better secure, aware, and prepared they are from and for security incidents. **Completion of training programs, completion of different practical exercises and drills**
Number of intrusion attempts	The number of intrusion attempts offers visibility into existing vulnerabilities and security measures in place.	The higher the number of intrusion attempts the larger the attack surface and the higher the chances of getting attacked. **The number of times the adversaries have tried to attack the system.**

Security incidents detected and resolved	The number of security incidents that were detected and resolved by the organization.	The higher the number of incidents detected and resolved the more prepared and vigilant the security team is. **Incidents in the past month/quarter/year**
Average cost to resolve	The average cost associated with resolving a security incident.	The lower the average costs, the better the financial effectiveness of the incident response efforts. **Avg. costs of resolving incidents monthly/quarterly/annually**
Repeated incidents	Number of security incidents that occur repeatedly within a specific timeframe.	This metric helps identify areas for improvement in incident response, security controls, and overall cybersecurity posture. **The number of repeated incidents monthly/quarterly/annually**
Devices with latest security patches	The percentage of the number of devices within an organization that has up-to-date security patches applied.	The higher the percentage, the better the organization's ability to maintain a strong security posture by promptly addressing known vulnerabilities and mitigating the risk of exploitation. **Percentage of devices**
High risk vulnerabilities	The number of high-risk vulnerabilities present in the organization's systems, applications, and infrastructure.	It helps identify and prioritize vulnerabilities that pose a significant risk to their security and require immediate attention. **The number of high-risk vulnerabilities over time (monthly, quarterly/annually)**
Frequency of backups	How often are backups of critical data and systems performed?	The more sufficient the backup schedule, the more organizations can enhance their incidence response capabilities, minimize data loss, and ensure business continuity. **Frequency of backup schedule (daily, weekly, monthly)**
Testing of incidence response plans	The frequency of testing activities conducted to evaluate the organization's incidence response plan.	It assesses the organization's preparedness, identifies gaps or weaknesses in the plan, and helps improve the overall incident response capabilities. **Frequency of testing activities (tabletop exercises, simulations, full-scale incidence response drills)**
Review and updates to security policy	The frequency of reviewing and updating the organization's security policies.	It reflects the organization's commitment to maintaining a current and robust set of policies that guide security practices and incident response efforts.

		The frequency of policy reviews and the number of policy updates made during each review
Devices running outdated/end-of-life software	The number or percentage of devices running software versions that are outdated or have reached their end-of-life (EOL) stage.	It reflects the organization's ability to maintain an updated software ecosystem, which is crucial for mitigating vulnerabilities and reducing the risk of security incidents. **The number/percentage of devices over time (monthly, quarterly/yearly)**
Frequency of risk assessments	How often are risk assessments conducted within an organization?	It reflects the organization's proactive approach to risk management and helps ensure that incident response efforts are aligned with the current threat landscape. **The frequency of risk assessments over a given period (monthly, quarterly, yearly)**

Conclusion

In conclusion, benchmarking cybersecurity response procedures for hospitals in Texas is a crucial step towards ensuring the protection of sensitive patient data and the overall integrity of healthcare systems. The ever-evolving nature of cyber threats necessitates a proactive approach that involves continuous evaluation and improvement of response protocols. By establishing benchmarks, hospitals in Texas can identify their strengths and weaknesses, compare their cybersecurity measures to industry standards, and adopt best practices to enhance their resilience against cyber threats. Through effective benchmarking, hospitals can prioritize investments in cybersecurity resources, training, and technologies, ultimately safeguarding patient privacy, maintaining the trust of the community, and ensuring uninterrupted delivery of critical healthcare services. By remaining vigilant and responsive, hospitals in Texas can serve as role models for other healthcare organizations, contributing to a stronger cybersecurity landscape in the healthcare sector as a whole.

References

[1] O. for C. Rights (OCR), "The Security Rule," *HHS.gov*, Sep. 10, 2009. https://www.hhs.gov/hipaa/for-professionals/security/index.html (accessed Apr. 07, 2023).

[2] O. for C. Rights (OCR), "HITECH Act Enforcement Interim Final Rule," *HHS.gov*, Oct. 28, 2009. https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html (accessed Apr. 07, 2023).

[3] "What is the HITECH Act? 2023 Update." https://www.hipaajournal.com/what-is-the-hitech-act/ (accessed Apr. 07, 2023).

[4] J. [D-N. Sen. Rosen, “S.3904 - 117th Congress (2021-2022): Healthcare Cybersecurity Act of 2022,” Oct. 18, 2022. http://www.congress.gov/ (accessed Apr. 07, 2023).
[5] C. for D. and R. Health, “Cybersecurity in Medical Devices Frequently Asked Questions (FAQs),” *FDA*, Mar. 2023, Accessed: Apr. 07, 2023. [Online]. Available: https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity-medical-devices-frequently-asked-questions-faqs
[6] “Texas Medical Privacy Act, Health Law & Policy Institute.” https://www.law.uh.edu/healthlaw/perspectives/privacy/010830texas.html (accessed Apr. 07, 2023).
-

INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security
Sam Houston State University

Gupta, K., Varol, C., & Shashidhar, N. (2023) Cyber- Security Threat: Benchmarking Cybersecurity Response Procedure for Hospitals in Texas. (Report No. IHS/CR-2023-1012). The Sam Houston State University Institute for Homeland Security. https://doi.org/10.17605/OSF.IO/Q2TFZ