Memo

**Memo: Identifying and Dealing with Ransomware Attacks**

**DATE:** March 1, 2025  
**FROM:** Hospital IT Department  
**TO:** All Company Employees  
**SUBJECT:** Critical Ransomware Security Alert and Prevention Protocols

**Background – Why should we be concerned about ransomware?**

Ransomware attacks are an increasingly prevalent risk to corporations around the world, but especially for those of us working in the medical industry. Hospitals in particular are threatened by these attacks to the sensitive nature of the data we store and utilize, and the real-time nature of the work done using this data.

For this reason, we have developed a new organizational ransomware policy to be adopted by all employees at our hospital. While employees are expected to familiarize themselves with the entirety of the new policy, this memo seeks to provide background information about ransomware threats to help you understand why these security measures are crucial to our operations and patient care.

**What is Ransomware?**

Ransomware is a type of malicious software that attacks a computer system by locking down access to all data and software within the system. Typically, this is done by encrypting the data. Hackers then demand a ransom payment to have the systems unencrypted or unlocked. These types of attacks are often accompanied by threats to leak or sell the sensitive data if the payment is not made within some time frame.

**How is Ransomware delivered?**

Ransomware is typically delivered to a target’s machine via a malicious link in a phishing email, visiting a compromised website, or exploiting vulnerabilities in other computer software. After clicking on a compromised link malicious software is downloaded to the computer. The ransomware software may then scan for other computers connected on the same local network and infect them as well.

For these reasons it is critical that you only click links in email from trusted sources. The same goes for attachments in any emails. Warning signs for these malicious emails are often poor grammar or misspellings, attachments you didn’t ask for, requests for sensitive or identifying information, a sense of urgency that you must act now, and offers that are too good to be true.

The protection section of our policy describes security measures including firewalls, anti-malware software, and network segmentation intended to prevent or limit the spread of ransomware software beyond its initial infection.

**Is Ransomware common?**

Unfortunately, ransomware is extremely common. According to Statista, there were nearly 500 million ransomware attacks in 2022 alone1. Similarly, the healthcare industry was the #1 target of ransomware attacks in the third quarter of 2024 receiving 18.6% of all attacks2.

**Ransomware Risks to Hospitals**

Hospitals face particularly difficult challenges when it comes to ransomware. Ransomware attacks can significantly disrupt hospital operations and impact patient care, including delays to treatment, distributors to diagnostic procedures, and potentially even the cancellation of scheduled surgeries.

Recovery from ransomware attacks can be devastating for a hospital. The cost of the ransomware payment, the downtime, and legal fees can easily amount to millions of dollars. In some cases it can even lead to the closure of a hospital. This was the case in 2023 for St. Margaret’s Health in Illinois. The hospital was unable to submit claims to insurers including Medicare and Medicaid for months.3 The downtime extended for over 14 weeks.

**Piedmont Hospital's Response**

To address the threats outlined above, Piedmont Hospital has developed an Organizational Ransomware Policy that follows the NIST Cybersecurity Framework’s guidelines and ensures HIPAA compliance. The policy outlines our governance structure, identification protocols, protection measures, detection abilities, response plan, and recovery playbook. All employees should familiarize themselves with the policy.

**References**

1. "Number of ransomware attempts per year 2023." *Statista*, Statista Inc.,<https://www.statista.com/statistics/494947/ransomware-attempts-per-year-worldwide/>. Accessed 25 Feb. 2025.
2. "Industries Impacted by Ransomware in the U.S. Q3 2024." *Statista*, Statista Inc.,<https://www.statista.com/statistics/1461346/ransomware-industries-affected-us/>. Accessed 25 Feb. 2025.
3. Dilanian, Ken. "Illinois Hospital Links Closure to Ransomware Attack." *NBC News*, 12 June 2023,<https://www.nbcnews.com/tech/security/illinois-hospital-links-closure-ransomware-attack-rcna85983>. Accessed 25 Feb. 2025.

Policy

Piedmont Hospital

Policy Manual

**Subject:** Organizational Ransomware Policy

**Approved By:** Piedmont Hospital IT Department (Group 25)

**Effective Date:** March 1, 2025

**Introduction**

Healthcare organizations are becoming targets to cyberattacks such as ransomware due to its accessibility to sensitive data such as patients’ health and financial records. Ransomware attacks can cause severe consequences such as disruptions in operations, financial losses, and legal repercussions. As a proactive approach, Piedmont Hospital has created a policy to help maintain a high standard of care while protecting patients, staff, hospital’s assets and infrastructure from cyberattacks.

This policy was established to protect the hospital’s infrastructure and data from ransomware threats. It is aligned to the best cybersecurity practices and standards that can be found in the National Institute of Standards and Technology Cybersecurity Framework. The policy provides guidance and procedures to decrease any chances of a ransomware attack while ensuring the compliance of the Health Information Portability and Accountability Act (HIPAA) and other healthcare regulations.

**Governance**

The governance structure for Piedmont Hospital IT department is designed to protect health information systems against attacks such as ransomware. The department is organized into specialized teams that are responsible for different levels of security such as network management, data protection, incident response, and compliance and is under the leadership of the following:

* **Chief Information Officer**-manages the organization's IT department and infrastructure while ensuring compliance of healthcare regulations such as HIPAA.
* **Chief Information Security Officer**- develops and implements security measures, responds to incidents.

These specialized groups of professionals regularly enhance their knowledge and skill sets through continuous education and they share this information by training other hospital employees on cybersecurity practices. Training often consists of routine phishing simulations and tutorials based on cybersecurity principles which can help enhance employees’ ability to recognize threats. All Piedmont Hospital employees are required to complete cybersecurity training annually.

**Identification**

In order to reduce our vulnerability to ransomware and any additional threats, the organization will regularly identify and evaluate its critical systems such as electronic health records, medical devices and any other infrastructure that is vital to the hospital operations.

Additionally, vulnerability assessments will be conducted monthly on all hospital systems. Automated tools will be deployed to identify security weaknesses such as outdated or unpatch software that can be exploited by ransomware. Vulnerabilities will be quickly resolved through software and system updates.

Sensitive data such as Protected Health information will be categorized according to sensitivity level. Additional security measures including strict access controls and data encryption will be implemented and only authorized personnel will have access to highly sensitive data.

The hospital will take proactive steps to mitigate these risks by monitoring external threats and interacting with experts within the security industry to stay informed of any potential ransomware attacks and best practices that are specific to the healthcare cybersecurity field. Additionally, the incident response team will be available to respond quickly when a threat occurs in order to minimize any potential damages.

**Protection**

To ensure the protection of its IT infrastructure and sensitive data from ransomware, the hospital will implement security protocols such as:

* Implementing firewalls and Intrusion Prevention systems to filter traffic and identify unusual activity within the networks. Networks that support patient records and other hospital systems will be segmented to prevent any ransomware from spreading into other areas in an event of an attack.
* Devices and systems will be equipped with up to date anti-virus and anti-malware software that goes through routine maintenance to ensure that vulnerable patches are in place. The data from these devices will be encrypted and stored in cloud based or data center locations which would allow quick retrieval during an incident.
* Role based access controls including multi-factor authentication to limit system access to authorized users.
* Cybersecurity training that covers several topics such as identifying social engineering and safe handling of confidential data will be available to all employees.

**Detection**

To prevent any form of manipulation and grow awareness of ransomware, the hospital advises all employees and clients to be sensitive to any potential threats. The security team aims to provide a safe environment for all personnel, patients, and new clients. In addition to these safety measures, the hospital is aware and implements a few methods to detect ransomware as soon as possible. With these reliable methods below, the hospital has the ability to detect any potential threats or compromise by analyzing any abnormal activity and creating plans to eliminate malicious situations.

* Firewalls: To increase the level of security, this is implemented to detect unknown TCP/IP packets of intrusion to prevent the risk of exposure in the local network. Internally, the security personnel execute an ongoing algorithm detecting any request made at any point of time. Depending on the packets and other network identifications, the firewall indicates if the method is safe or an act of ransomware.
* Intrusion Detection System: The Intrusion Detection System (IDS) is an alerting program that sends alerts and escalates the interference directly to management and the security team when the system encounters a compromise. Afterwards, the hospital management and security will control the situation once they are notified.
* Log Monitoring: In order to have full details of the events, the log monitoring coordinates the IDS to ensure that all communication into and out of the hospital is recorded and stored in a monitoring system. Every type of request being sent into the local area network interface is documented to identify inappropriate attempts of ransomware.
* Secure Shell: In order to enter an internal system, the implementation of Secure Shell (SSH) is enforced so only select individuals, or IP addresses, have access to internal databases, servers, and systems.

**Response**

At the time of a potential ransomware attack, a strict guide is to be followed to limit a greater exposure to the system. This is to be followed by the security team and any other influence acting against the ransomware. Below is the response plan to counter plausible accounts:

* It is critical that all individuals affected by an incident are immediately notified that personal, medical data may have been compromised as well as an immediate action plan to recover security and information.
  + At the beginning of the ransomware attack, there will only be an individual notice to the affected individuals. After the issue has been resolved, all businesses and individuals involved with the hospital will be notified that a breach has occurred but is urgently being recovered.
* The security team must proceed to minimize a large threat under all HIPAA guidelines. All members of the hospital are required to be trained if an electronic or physical breach were to occur.
* As soon as an incident is suspected, the incident is immediately escalated to the correct security team on duty using the IDS. The situation and all forms of communication of the ransomware incident will be handled by management and the security team. Information from management and security will be limited to avoid additional breaches of personal health data.
* In addition to the security and management team, the IT department will also be investigating services and operations the hospital must pause or proceed during a ransomware attack. Depending on the type of attack, the IT team has authority to cease services that are affected by the ransomware. If a direct service or operation is not affected by the attack, then it can continue its normal procedure with highly attentive care. Systems that are directly impacted by ransomware will be managed appropriately by IT.
* Depending on the situation, management and the security team will decide to accept the ransomware risk or to engage with the ransomware attack. At this time, they will determine what is the best and most effective response to the attack.
  + If the ransomware is at a critical risk and no attempt to recover is possible, the result will be a direct loss on behalf of the hospital, meaning that we have accepted the terms and conditions of the ransomware.
  + Otherwise, the team will combat all potential threats and vulnerabilities lowering the likelihood and impact of exposed data and systems.

When a ransomware incident is detected, staff must immediately report it to the security team with all relevant details including logs and observed anomalies. It is important to provide every possible detail that could be obtained to give the most transparent interpretation to the analysis. The team will continue to investigate any given intrusion until the ransomware is found in a timely manner.

**Recovery**

Following any type of intrusion, the security and management are tasked to do an urgent restoration of personal data, including medical and personal information. Using backups of data and software, all systems should be restored without delay. The priority after the incident is to resume all nominal operations as soon as possible.

Additionally, all affected parties of a ransomware attack should be alerted immediately with a well detailed sequence of events, such as a post-mortem report. This post-mortem documentation is a combination of the risk analysis and risk assessment; it discusses in fine detail the sequence of events, any services affected, the decision, the impact, and the likelihood of the risk.

All devices or data systems will be restored as well as updated to the newest version in order to improve reliability and assurance within the organization, including patients. Each system affected will also have its own individual report and procedure by raising defense costs to minimize the probability of a vulnerable compromise.

If any of the affected parties are damaged financially from an incident, the hospital is to take full responsibility to renew any financial repayment urgently. All financial payments that are needed to be replenished need to report to the hospital as soon as possible within reasonable time.

After an incident, the hospital will introduce a descriptive analysis to prevent such ransomware in the future within 30 days of the incident to select individuals.

**Conclusion**

The hospital and its policy is intended to comply with industry regulations, standards such as HIPAA and any state laws that are relevant to the breach of data notification. This policy will be reviewed annually to ensure the hospital is aligned with the most current changes in industry standards and new threats.

**References**

1. US Department of Health and Human Services. *HIPPA For Professionals.* US Department of Health and Human Services. <https://www.hhs.gov/hipaa/for-professionals/index.html>
2. US Department of Health and Human Services. *Ransomware Fact Sheet.* US Department of Health and Human Services, 2021 <https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/ransomware-fact-sheet/index.html>
3. US Department of Health and Human Services. *Top 10 Tips for Cybersecurity*. US Department of Health and Human Services, 2018 <https://www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf>
4. American Hospital Association. “A Look at 2024’s HealthCare Cybersecurity Challenges.” American Hospital Association, October 2024, <https://www.aha.org/news/aha-cyber-intel/2024-10-07-look-2024s-health-care-cybersecurity-challenges>
5. National Institute of Standards and Technology. NIST Cybersecurity Workforce Framework. NIST, 2020, <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>
6. Baker, Kurt. “How Ransomware Spreads.” CrowdStrike. 5 October 2023. <https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/how-ransomware-spreads/>
7. US Department of Health and Human Services for Civil Rights. *HIPAA Administrative Simplification*. US Department of Health and Human Services. March 2013. <https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf>
8. US Department of Health and Human Services. *Breach Notification Rule*. US Department of Health and Human Services. <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>

Brainstorming Notes

Piedmont Hospital in Atlanta

1968 Peachtree Rd NW, Atlanta, GA 30309

MLA format throughout

(Hayden) Hospital ransomware news articles that I dug up from the tech community:

* [Illinois Hospital First To Shut Down Completely After Ransomware Attack | Techdirt](https://www.techdirt.com/2023/06/16/illinois-hospital-first-to-shut-down-completely-after-ransomware-attack/)
* [Cybereason: 80% of orgs that paid the ransom were hit again | VentureBeat](https://venturebeat.com/security/cybereason-80-of-orgs-that-paid-the-ransom-were-hit-again/)
  + 80% of hospitals that paid were hit again
* FBI takedown of prominent group: [U.S. Department of Justice Disrupts Hive Ransomware Variant](https://www.justice.gov/archives/opa/pr/us-department-justice-disrupts-hive-ransomware-variant)

(Hayden) Some notes from the 2/14 office hours:

* **The ransomware security policy assignment should be written from the perspective of different hospital employees.** This means that students should consider how the policy will be interpreted and implemented by different staff members, such as doctors, nurses, and administrators.
* **The policy should consider the target audience.** The target audience for the policy is all hospital employees, as well as third-party vendors and other stakeholders.
* **The policy should be ‘actionable’.** Can the hospital still deliver care to the patients in the hospital, especially the critical care patients? Do the doctors and nurses know what to actually do?
* **The policy should avoid repeating specific policy elements from other policies.** This means that students should not simply copy and paste from other policies, but should instead focus on writing a clear and concise policy that is specific to ransomware.
* **The policy should be clear and concise.** The policy should be easy to read and understand, and should not be unnecessarily long or complex.
* **Students should look at some regulations and what they require in terms of ransomware security.** This will help students to understand the legal and regulatory landscape surrounding ransomware, and to develop a policy that is compliant with applicable laws and regulations.

(Hayden) A primer on ransomware and some details related to hospitals. I created this using the deep research functionality of Google Gemini: [Ransomware Policy Research for Hospitals](https://docs.google.com/document/d/1RGsE4BBZLtqR1iYrCRFVROGQjG0O3477lGBpqNn2Uhc/edit?usp=sharing)

(Hayden) We have to cover Governance, Identification, Protection, Detection, Response and Recovery.

The CSF Core Functions — GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, and RECOVER — organize cybersecurity outcomes at their highest level.

• GOVERN (GV) — The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored. The GOVERN Function provides outcomes to inform what an organization may do to achieve and prioritize the outcomes of the other five Functions in the context of its mission and stakeholder expectations. Governance activities are critical for incorporating cybersecurity into an organization's broader enterprise risk management (ERM) strategy. GOVERN addresses an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policy; and the oversight of cybersecurity strategy.

-Include governance structure such as CIO, CISO, IT response team and explain training for employees

• IDENTIFY (ID) — The organization's current cybersecurity risks are understood. Understanding the organization's assets (e.g., data, hardware, software, systems, facilities, services, people), suppliers, and related cybersecurity risks enables an organization to prioritize its efforts consistent with its risk management strategy and the mission needs identified under GOVERN. This Function also includes the identification of improvement opportunities for the organization's policies, plans, processes, procedures, and practices that support cybersecurity risk management to inform efforts under all six Functions.

-possible vulnerable systems/assets for our assignment: electronic health records, medical devices

• PROTECT (PR) — Safeguards to manage the organization's cybersecurity risks are used. Once assets and risks are identified and prioritized, PROTECT supports the ability to secure those assets to prevent or lower the likelihood and impact of adverse cybersecurity events, as well as to increase the likelihood and impact of taking advantage of opportunities. Outcomes covered by this Function include identity management, authentication, and access control; awareness and training; data security; platform security (i.e., securing the hardware, software, and services of physical and virtual platforms); and the resilience of technology infrastructure.

-implement firewalls, network segmentation that was mentioned in the lecture, MFA

• DETECT (DE) — Possible cybersecurity attacks and compromises are found and analyzed. DETECT enables the timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse events that may indicate that cybersecurity attacks and incidents are occurring. This Function supports successful incident response and recovery activities.

-IDPS (mentioned in the lectures), log monitoring, etc

• RESPOND (RS) — Actions regarding a detected cybersecurity incident are taken. RESPOND supports the ability to contain the effects of cybersecurity incidents. Outcomes within this Function cover incident management, analysis, mitigation, reporting, and communication.

• RECOVER (RC) — Assets and operations affected by a cybersecurity incident are restored. RECOVER supports the timely restoration of normal operations to reduce the effects of cybersecurity incidents and enable appropriate communication during recovery efforts.

-backups/data recovery

<https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/ransomware-fact-sheet/index.html>

<https://www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf>

<https://www.aha.org/news/aha-cyber-intel/2024-10-07-look-2024s-health-care-cybersecurity-challenges>

<https://press.un.org/en/2024/sc15891.doc.htm>

Three rules of HIPPA: 1) Privacy Rule, 2) Security Rule 3) Enforcement/Breach Notification Rule  
<https://www.hhs.gov/hipaa/for-professionals/index.html>

To do:   
1) Choose a hospital:

2) Determine how we split it up:  
Possible ways to split: one person do the memo (Hayden), one person do Governance, Identification, Protection (Dasaray), one person do Detection, Response and Recovery (Nataly) (just a suggestion, feel free to provide any thoughts/changes)