1 Purpose

1.1 Federal and State laws, as well as organizational policies, describe measures to safeguard sensitive information to include Protected Health Information (PHI/ePHI). Unauthorized individuals who access, use, and/or disclose sensitive data to include PHI, attempt to access sensitive data, and/or assist others to access sensitive when it is not authorized will be sanctioned appropriately.

1.2 This policy has been implemented to establish guidance for prevention and response of malware attacks, commonly known as Ransomware, for all computers connected to [Company Name] information.

1.3 Applicability – This policy applies to all [Company Name] workforce members, contractors, interns and anyone working with or utilizing [Company Name] information systems, collectively referred to as workforce members.

2 Policy

2.1 This policy is intended to work with the Incident Response Policy and associated response plans but provides more detailed guidance focused on preventing and addressing ransomware incidents. An Incident, as it pertains to cybersecurity, is any activity that harms or threatens [Company Name]'s IT infrastructure in whole or in part.

2.2 Ransomware incidents can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services. Reported incidents of ransomware criminals targeting Healthcare have continued to increase and ransomware represents a significant risk to [Company Name] and patient data.

2.3 Ransomware attacks are designed to block access to computer systems by encrypting data, making it unreadable, and then demanding a 'ransom', usually in the form of money, forrestoring access to the system or data.

2.4 Payment of ransoms should be considered as an option to restore access to otherwise blocked data. However, restoration of data is typically only successful in <50% of reported cases. Some studies indicate the success rate is closer to 20%. Regardless of whether a ransom is paid, the infected machine should be removed from use and reimaged.

2.5 [Company Name] personnel are responsible for protecting [Company Name] IT systems to prevent and mitigate ransomware incidents. Prevention and effective response to the ransomware threats require a broad response which [Company Name] 's IT Security Policies are designed to address along with other cyber threats.

2.6 Employees should immediately report suspected ransomware incidents to the Helpdesk, who will initiate the Incident response plan & notify the CISO and Compliance Officer.

2.7 Operational Preparedness / Prevention

Prevention of ransomware will include the following activities:

- Security awareness training, including ransomware content
- Social engineering training
- Strong email security (as determined by the CTO)
- Current Antivirus software
- Maintain a Ransomware Plan
- Ensure insurance policies specifically address this attack type
- Establish and test the business continuity/contingency plan
- Develop a Communication Plan to include workforce, patients, vendors, media, insurance, legal, Law Enforcement, State and Federal authorities
- Create a Public Relations (PR) plan

2.8 Technical Preparedness:

1. Installation of current security patches for Operating Systems and Applications
2. Current inventory of hardware and software
3. Business impact analysis with recovery time and recovery point determinations
4. Periodic vulnerability scans of IT systems
5. Removal of unused/unlicensed software
6. Establish and test online and offline backups for all data and systems
7. Enforce least privilege access to data storage
8. Establish file & log security and monitoring capabilities
9. Current connectivity diagrams
10. Secure design of all IT systems, including networked biomedical devices
11. Consider disabling windows scripting (JavaScript & VBScript) and Flash

3 Equipment/Software

All [Company Name] information systems, data, hardware and applications.

4 General Procedures

4.1 Prevention

4.1.1 Internet-Facing Vulnerabilities

1. Conduct regular vulnerability scanning to identify and address

vulnerabilities, especially those on internet-facing devices, to limit the attack surface.

2. Regularly patch and update software and OSs to the latest available versions.
3. Implement filters at the email gateway to filter out emails with known malicious indicators, such as known malicious subject lines, and block suspicious Internet Protocol (IP) addresses at the firewall.
4. To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification. DMARC builds on the widely deployed sender policy framework and Domain Keys Identified Mail protocols, adding a reporting function that allows senders and receivers to improve and monitor protection of the domain from fraudulent email. Ensure devices are properly configured and that security features are enabled.
5. Employ best practices for the use of RDP and other remote desktop services.
6. Disable or block Server Message Block (SMB) protocol outbound and remove or disable outdated versions of SMB. Threat actors use SMB to propagate malware across organizations. Based on this specific threat, organizations should consider the following actions to protect their networks:

a. Disable SMBv1 and v2 on your internal network after working to mitigate any existing dependencies (on the part of existing systems or applications) that may break when disabled.

   i. - Remove dependencies through upgrades and reconfiguration: Upgrade to SMBv3 (or most current version) along with SMB signing.

b. Block all versions of SMB from being accessible externally to your network by blocking TCP port 445 with related protocols on User Datagram Protocol ports 137–138 and TCP port 139

4.1.2 Phishing Vulnerabilities

1. Implement a cybersecurity user awareness and training program that includes guidance on identifying and reporting suspicious activity (e.g., phishing) or incidents.
2. Conduct organization-wide phishing tests to gauge user awareness and reinforce the importance of identifying potentially malicious emails.

4.1.3 Malware Infection

a. Ensure antivirus and anti-malware software and signatures are up to date. Additionally, turn on automatic updates for both solutions.

b. Use application directory allow listing on all assets to ensure that only authorized software can run, and all unauthorized software is blocked from executing.

   i. Enable application directory allow listing through Microsoft Software Restriction Policy or AppLocker.

   ii. Use directory allow listing rather than attempting to list every possible permutation of applications in a network environment. Safe defaults allow applications to run from PROGRAMFILES, PROGRAMFILES(X86), and SYSTEM32. Disallow all other locations unless an exception is granted.

4.2 Detection of Ransomware:

1. Implement an intrusion detection system (IDS) to detect command and control activity and other potentially malicious network activity that occurs prior to ransomware deployment.

Common scenarios where a ransomware attack is indicated:

2. **Inability to access certain files**, locally and on the network, **as the ransomware encrypts, deletes and renames and/or relocates data**. This is typical behavior of ransomware to create confusion on which file is affected.

3. **File Renaming**

   When ransomware gets into your computer, it renames your data. This is one way of identifying ransomware on your computer. **Users receive a message notifying them of a ransomware attack.** A userreceived a pop-up message notifying them their files have been encrypted and providing instructions to pay a ransom. Many times, the user will be unable to access their computer. A related attack is when a user receives a ransom email or message indicating some level of access was obtained and requests a ransom to avoid some sort of negative impact.

Sample Message

4.3 Response

As with most IT-related security incidents, a well-planned and executed response can greatly reduce the impact and cost of a ransomware attack. An improper response can likewise greatly increase the cost and result in the spread of ransomware within the organization.

The following steps should be followed when a ransomware incident is suspected:

1. Open a tracking ticket.
2. Notify CISO and Compliance Officer of a suspected Security Incident.
3. Complete the five phases for the ransomware response.
    a. Analysis
    b. Containment
    c. Eradication
    d. Recovery
    e. Post-Incident Analysis
4. Perform the Security Incident Response Plan and Notifications if required.

4.3.1 Five Phases for the Ransomware Response

1. Analysis/Identification

- Identify the systems and accounts involved in the initial breach. Identification of the ransomware is important to identify its capabilities. Most variants spread via email or a web browser.
- Identify the ransomware variant. Each ransomware variant has characteristics which can be used to identify the specific version. New variants are discovered on a regular basis, so research should be done at the time of the event based on the observed characteristics. Methods useful for identifying the ransomware version:
    a. an inability to access certain files as the ransomware encrypts, deletes and renames and/or relocates data; and Ransomware message
    b. Numerous online ransomware detection tools exist which will identify the strain.
    c. Research file type, aka, internet search.
    d. Third party websites such as https://id-ransomware.malwarehunterteam.com/
    e. Some variants have free keys available from security organizations to restore access
- Source Determination –Once inside an organization, many will spread via network connectivity. It is essential to understand how the ransomware entered the environment. A more formal analysis should be completed after the incident has been addressed.

2. **Containment**

Once a system has been identified as having ransomware, the potentially infected computer should be quickly isolated from the network (including WIFI) to prevent further spread of the malware. The goal of containment is to stop the spread of ransomware and encryption of additional files. Containment methods can vary depending on the version of ransomware identified. Methods of containment include:

a. Isolate the computer from any network connection, including WIFI
b. Shutdown the computer
c. Set the computer to hibernate
d. Stop access to file shares
e. Restrict by network or firewall
f. It's not recommended to change permissions on files within a share due to propagation times.
g. If ransomware is identified on a file server, it is not normally

necessary to shut the server down if the above steps are used.

h. Verify backups and scan for the malware.

i. Determine if paying the ransom is required to retain the data (see the Ransomware Decision Guide).

3. Eradication

Any system confirmed as being infected with ransomware must be rebuilt from a known good source. Preservation of data is the key consideration, NOT preservation of the existing system build. Even if the decision was made to pay the ransom, these steps should be taken to prevent continued infections:

a. Complete a malware scan of the organization.

b. If the ransomware was email-based, complete a search and purge all similar messages. Examine systems which may have received the email.

c. If the ransomware was web browser-based, block the suspect sites. Review and update vulnerable browser components.

d. Perform vulnerability scans and patch vulnerable operating systems and applications

e. Change passwords for the affected users

f. Secure the network and other information sources from continued credential-based unauthorized access may include the following actions:

- Disabling virtual private networks, remote access servers, single sign-on resources, and cloud-based or other public-facing assets.

4. **Recovery**

Recovery from ransomware typically requires rebuilding of the infected machines and restoration of data. If the incident requires notification, those processes should be initiated according to the Incident Response Plan.

5. Post-Incident Analysis

Conduct post-incident activities, which could include a deeper analysis of the evidence to determine if the entity has any regulatory, contractual or other obligations resulting from the incident (such as providing notification of a breach of protected health information. Post-incident Analysis includes:

a. Fully documenting the incident.

b. Identifying what detection and security controls were in place to help.

c. Identifying detection and security controls that would help to prevent future impacts.

d. Determine if additional End User training necessary.

e. Determine if the entity has any regulatory, contractual or other obligations as a result of the incident.

f. Hold a review meeting to identify new ways to detect, respond, analyze, and prevent similar incidents.

g. Review lessons learned, incorporating any lessons learned into the overall security management process to improve incident response effectiveness for future security incidents

4.4 Paying the Ransom

The **Ransomware Decision Guide** is intended to provide the decision points to assist in determining whether it is necessary to pay the ransom. While paying the ransom may appear to be a much cheaper solution in the short term, it does not have a good history of being effective. Paying the ransom only results in restoration of the data between 19% and 50% of the time. More often, the attacker provides the incorrect key or does not provide one at all. The cost and labor of containing and eradicating the malware will still need to be performed.

If viable backups do not exist, the only option of regaining access to the data may be to pay the ransom.

4.5 Incident Reporting:

In the case of an incident, as defined in this policy, all entities must follow the procedures found in [Company Name] 's Incident Response and Reporting Plan.

All Incidents, threats, or violations that affect or may affect the confidentiality, integrity, or availability of ePHI must be reported and responded to in accordance with this policy, the Incident Response Policy and the Incident Response Plan.

All HIPAA-Security related incidents and their outcomes must be logged, documented and maintained according to the Incident Response Plan.

Any individual who believes that an incident has occurred is to immediately notify XXXXXX via XXXXXX.

4.6 Confidentiality

All information related to an electronic or physical security incident must be treated as confidential information until the incident is fully contained. This will serve both to protect employees' reputations (if an incident is due to an error, negligence, or carelessness) and control the release of information to the media and/or customers.

5 Attachments

Not Applicable

6 References and Related Documents / Forms

§164.308(a)(6)(i) Security Incident Procedures

§164.308(a)(6)(ii) Response and Reporting

7 Revisions

Document Title:	**Ransomware Prevention and Response Policy**		**Revision No.:**	**1.0**
Department:		RevisionDate:		
Author:		Date Created:		
Approved By:		Date Approved:		
Approved By:		Date Approved:		

CHANGE HISTORY

EffectiveDate	Version	Change Summary	Change Approval
	1.0	New Policy	