Document Title:	Ransomware Prevention and Response Policy	Revision No.:	2.0
Department:		Revision Date:	Click here to enter a date.
Author:		Date Created:	Click here to enter a date.
Approved By:		Date Approved:	Click here to enter a date.
Approved By:		Date Approved:	Click here to enter a date.

CHANGE HISTORY

Effective Date	Version	Change Summary	Change Approval
			Click here to enter a date.
			Click here to enter a date.
			Click here to enter a date.
			Click here to enter a date.
			Click here to enter a date.

Purpose:
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 PHI, attempt to access PHI, and/or assist others to access PHI when it is not authorized will be sanctioned appropriately. This policy has been implemented to establish guidance for prevention and response of malware attacks commonly known as Ransomware for all computers connected to the ABC Corporation, LLC (ABC) information.

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

Ransomware is a type of malicious software designed to block access to a computer system until a sum of money is paid. Reported incidents of ransomware criminals targeting Healthcare have continued to increase and ransomware represents a significant risk to ABC and patient data.

Ransomware attacks are designed to block access to computer systems by encrypting data and then demanding a 'ransom', usually in the form of money, for restoring access to the system or data. Ransomware attacks can be minor or in some cases cause a significant adverse impact to ABC operations and patient care. In some cases, successful attacks have resulted in loss of access to EHR systems, other IT systems, and patient data.

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.

ABC personnel are responsible for protecting ABC IT systems for the prevention and mitigation of ransomware incidents. Prevention and effective response to the ransomware threat requires a broad response which ABC's IT Security Policies are designed to address along with other cyber threats.

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

Operational Preparedness / Prevention:
Prevention of a 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 a business continuity / contingency plan
- Develop a Communication Plan to include workforce, patients, vendors, media, insurance, legal, Law Enforcement, State and Federal authorities
- Create a PR plan

Technical Preparedness:

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

Procedure:

Detection of Ransomware:

Common scenarios where a ransomware attack is indicated:

1. **files on a network file share are unexpectedly encrypted** – Usually the most severe type of ransomware attack as it indicates there is an infected computer on the network. These types of attacks usually have the capability of effecting the most data throughout the network.

2. **files on a local computer are unexpectedly encrypt**ed – Users may attempt to access files and find them encrypted but they have not received a message. Frequently there are delays built into ransomware which are designed to allow time for the broadest infection of the malware.

3. **users receive a message notifying them of a ransomware attack** – A user received 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

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. Improper response can likewise greatly increase the cost and result in the spread of the 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

1. Analysis

- **Identification –** Rapid identification of the ransomware variant is critical. 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:
    - Ransomware message
    - Numerous online tools exist which will identify the strain.
    - Check file extension using Google
    - Third party websites such as https://id-ransomware.malwarehunterteam.com/
    - Some variants have free keys available from security organizations to restore access

- **Source Determination –** Identification of the ransomware is important to identify its capabilities. Most variants spread via email or via a web browser. 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 the 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. Remove shares
    f. Restrict by network or firewall
    g. It's not recommended to change permissions on files within a share due to propagation times.
    h. If the ransomware is identified on a file server it is not normally necessary to shut the server down if the above steps are used.
    i. Verify backups and scan for the malware
    j. Determine if paying the ransom is required to retain the data (see the Ransomware Decision Guide)

3. **Eradication –** Any system which has been 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

4. **Recovery -** Recovery from ransomware typical 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**
    a. Ensure the incident is fully documented
    b. Review lessons learned
    c. What detection and security controls were in place to help?
    d. What detection and security controls would have helped to prevent?
    e. Is additional End User training necessary?
    f. Hold a review meeting for the purpose of identifying new ways to detect, response, analyze and prevent similar incidents.

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 20%

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.

Incident Reporting:
In the case of an incident as defined in this policy, all entities must follow the procedures found in ABC'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 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.

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 to control the release of information to the media and/or customers.

RELEVANT REFERENCES:

§164.308(a)(6)(i) Security Incident Procedures
§164.308(a)(6)(ii) Response and Reporting