Prepare, React, and Recover from Ransomware

Every healthcare organization, regardless of size, is a potential target for Ransomware attacks. Preparing for, preventing, and recovering from Ransomware attacks is paramount to patient safety. Follow these industry tested best practices (Prepare, React, Recover) to ensure your organization is prepared for these attacks and can continue to keep patients safe in the event of an attack.

Acronyms

CISA—Cybersecurity and Infrastructure Security Agency
HHS—United States Department of Health and Human Services
ISAC—Information Sharing and Analysis Center
ISAO—Information Sharing and Analysis Organizations
MS-ISAC—Multi-State Information Sharing and Analysis Center

	GENERAL USERS AND MEDICAL PRACTITIONERS	CYBER/IT PROFESSIONALS	EMERGENCY MANAGERS
PREPARE Before the attack	• Practice pen and paper operations to maintain hard copies of patient data • Understand your organization's incident response plan • Identify your IT/Security point of contact in case of a cyberattack	• Maintain offline, encrypted backups of data with 3-2-1 backup strategy • Create, maintain, and exercise a cyber incident response plan to include a communication strategy during incidents • Conduct regular vulnerability scanning • Regularly patch and ensure devices are securely configured. • Apply the principle of least privilege to all systems and devices • Implement security protocols and filters at the email gateway to prevent successful phishing attempts • Authenticate in-bound email to prevent email spoofing	• Perform risk management for third party vendors and managed service providers (verify) • Implement a cybersecurity user awareness and training program • Make sure you understand which personnel will support the leader during each phase of the investigation
REACT During the attack	• Implement your organization's protocol for incident handling • Consider removing the ability to print and copy/paste from Electronic Medical Records (EMR) applications or web mail accessed from home	• Implement steps learned in your cybersecurity awareness and training program • Request assistance from CISA, HHS, MS-ISAC, and local, state, or federal law enforcement partners • Take a system image and memory capture of a sample of affected devices and collect relevant logs for evidence • Consult federal law enforcement about possible decrypts available and follow trusted guidance for the particular ransomware variant	• Determine which devices were affected and immediately isolate them • Power down affected systems for investigation and recovery • Triage affected systems for investigation and recovery • Contain any associated systems that may be useful for further or continued unauthorized access
RECOVER After the attack	• Take care not to reinfect clean systems during recovery • Document lessons learned and adjust policies and response plans accordingly	• Restore data from offline, encrypted backups based on prioritization of critical services • Issue password resets for all affected systems and users • Follow additional technical guidance from CISA and MS-ISAC • Monitor network traffic and run antivirus scans to identify any remaining infection • Address any associated vulnerability and gaps in security or visibility • Clean, rebuild, and re-connect systems based on prioritization of critical services	• Confer with team and stakeholders to document what happened on initial analysis • Consider sharing lessons learned and indicators of compromise with CISA or your sector ISAC/ISAO for further sharing and to benefit others within the community

Health Sector Cybersecurity Coordination Center (HC3) was created by the Department of Health and Human Services to aid in the protection of vital, healthcare-related controlled information and ensure that cybersecurity information sharing is coordinated across the Health and Public Health Sector (HPH).

To learn more and access HC3 resources you can visit their site, here.

*To learn more about how you can protect your patients from cyber threats check out the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication. Check out the available resources 405(d) has to offer by visiting our social media pages: **@ask405d** on Facebook, Twitter, LinkedIn and Instagram! And check out our new website at 405d.hhs.gov!*