IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

RESPONDING TO RANSOMWARE: A GUIDE TO HEALTHCARE ORGANIZATIONS

STOP RANSOMWARE

This guide has been developed by the Cybersecurity & Infrastructure Security Agency (CISA) to help healthcare organizations be prepared to respond to potential ransomware attacks.

This guide is a template. Ransomware may disrupt access to online copies, so this is designed to be filled in, printed out, and kept handy in case of an incident to hasten decision-making and response. Primary point-of-contact name, work number and/or mobile number. Use sticky notes for additional contacts.

Key operational, support, and leadership contacts during an event or incident	
Incident Commander (leads response and escalation)	Tech Partners (ISP, Incident Response, Backup, MSSP, Email)
Chief Counsel (legal and compliance workstreams)	Clinical Partners (Biomed, EMR)
Public Relations (inbound and outbound comms)	CISA (assist in response and recovery) CENTRAL@cisa.dhs.gov
Executive Officer (incident declaration)	Insurer (provide resources and recommend providers)
Clinical Leadership (CMO, CMIO, CNO)	Law Enforcement (FBI, Secret Service, Local)

Key planning, reporting, and post-incident contacts after recovering from an event or incident	
Insurer(s) (revisit coverage types and levels)	**Health ISAC**
Health and Human Services	CISA Regional Advisor (preparation and prevention)
State Health Authorities	Tech Partners (preparation and prevention)
Location of SOP Binder	Last update of SOP Binder

KEY STEPS/CONSIDERATIONS TO PRESERVE PATIENT CARE:

- Do you have a checklist of items to prepare before visiting the Ransomware site and starting the timer that triggers subsequent stages of the attack?
- What is the date of the last downtime drills in the case of Ransomware, and have you addressed significant clinical impacts?
- What was the last date backup restoration of critical systems was confirmed?
- Do any of your insurance policies specifically cover or exclude Ransomware-related events?
- Do you have decision trees for who makes which decisions at which conditions and thresholds, including disconnecting clinical or other systems to prevent Ransomware spread?

For more resources, visit https://www.cisa.gov/stopransomware/healthcare-and-public-health-sector.