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

<table>
<thead>
<tr>
<th>Contact Type</th>
<th>Contact Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Commander (leads response and escalation)</td>
<td>Tech Partners (ISP, Incident Response, Backup, MSSP, Email)</td>
</tr>
<tr>
<td>Chief Counsel (legal and compliance workstreams)</td>
<td>Clinical Partners (Biomed, EMR)</td>
</tr>
<tr>
<td>Public Relations (inbound and outbound comms)</td>
<td>CISA (assist in response and recovery) <a href="mailto:CENTRAL@cisa.dhs.gov">CENTRAL@cisa.dhs.gov</a></td>
</tr>
<tr>
<td>Executive Officer (incident declaration)</td>
<td>Insurer (provide resources and recommend providers)</td>
</tr>
<tr>
<td>Clinical Leadership (CMO, CMIO, CNO)</td>
<td>Law Enforcement (FBI, Secret Service, Local)</td>
</tr>
</tbody>
</table>

Key planning, reporting, and post-incident contacts after recovering from an event or incident

<table>
<thead>
<tr>
<th>Contact Type</th>
<th>Contact Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insurer(s) (revisit coverage types and levels)</td>
<td>Health ISAC</td>
</tr>
<tr>
<td>Health and Human Services</td>
<td>CISA Regional Advisor (preparation and prevention)</td>
</tr>
<tr>
<td>State Health Authorities</td>
<td>Tech Partners (preparation and prevention)</td>
</tr>
<tr>
<td>Location of SOP Binder</td>
<td>Last update of SOP Binder</td>
</tr>
</tbody>
</table>

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?