Healthcare System Cybersecurity Incident Readiness and Response Considerations Working Draft

Cyber Incident Response Checklist

Immediate Response Activities

- Identify working communication capabilities (e.g., phone systems, portable radios, mobile communication applications, low voltage clinical cell phone(s), PA systems).
- Create a generic incoming message for phone systems. Post updates on websites, intranet, and Emergency Alert Systems such as crawlers, social media pages.
- Ascertain status of diagnostic and biomedical equipment function; implement downtime procedures when appropriate.
- Determine if any hospital or outpatient services will need to be altered; consider postponing elective surgeries, diagnostic procedures, and clinic visits.
- Identify external areas that require attention, such as electronic signs, parking garages, diverting traffic, posting signs, monitoring, or closing entrances/exits. Monitor environmental systems (e.g., heating, ventilation, air conditioning, and utilities) for proper function.
- Establish contact with IT vendors and cyber insurance representatives, to discuss response management and recovery support options. Technical vendors may provide backup services, assist with re-establishing network connectivity, or provide essential equipment, and resources.
- Consider what other partner organizations or facilities need to be briefed. If the disruption is deemed intentional or targeted, contact local law enforcement and appropriate Federal agencies (Department of Homeland Security, Federal Bureau of Investigation) and State/local cyber terrorism divisions as appropriate.

General Response Considerations

- Clearly communicate the scale and expected duration of the incident to staff so they plan appropriately and alter workflows as needed. Staff recognizing the severity of a cyber event leads to greater compliance with downtime procedures and recovery efforts. It also decreases stress, frustration, and anxiety.
- Ensure the IMT, or other proper chain of command, is effectively delegating tasks and tracking requests status to avoid duplicate requests to multiple teams thereby wasting manpower. Check-on ancillary groups (e.g., ambulatory) to assess their needs and have them implement pertinent DT procedures and form utilization.
- Identify necessary personnel for 24/7 key services. Identify who will be required onsite and who can work from home. Determine if the appropriate equipment is available for staff moving offsite. Appoint a representative and backup from each department (including ancillary services), as possible, to voice issues/concerns, engage with Incident Command Section leadership, and serve as liaison during the incident response and recovery stages.
- Consider additional officer/personnel presence (stationary vs rounding) in high-risk areas. Implement necessary security procedures for securing access if badging systems are down. Utilize sign-in sheets to track visitation and external workers (e.g., utility workers, repairmen).
- Address ordering for nutrition, cleaning, linen services; resupply of medical and non-medical items with appropriate vendors.