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).
- ☐ Send automated alert to staff and affected facilities. Clearly communicate the scope, impact, and estimated duration of the event. Include external partners (e.g., first responders, ancillary departments, and vendors).
- ☐ Create a generic incoming message for phone systems. Post updates on websites, intranet, social media pages, and Emergency Alert Systems.
- ☐ Ascertain status of diagnostic and biomedical equipment; implement downtime (DT) procedures when appropriate. Immediately disconnect possibly impacted equipment to limit scope of the attack.
- ☐ Determine if any hospital or outpatient services will need to be altered; consider postponing elective surgeries, diagnostic procedures, or clinic visits. Consider if hospital diversion will be necessary; identify and contact transfer centers. Develop external messaging in case of transfer or altered services; consider special needs of patients being transferred.
- ☐ Identify external areas that require attention, such as electronic signs, parking garages, traffic signs, or those related to monitoring or closing entrances/exits. Monitor environmental systems (e.g., heating, ventilation, air conditioning, and other 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 (U.S. Department of Homeland Security, Federal Bureau of Investigation) and state/local cyber terrorism divisions as appropriate. Consider utilizing H-ISAC as a primary contact for assistance.

General Response Considerations

- ☐ 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 and who will be required onsite and who can work remotely. Determine if the appropriate equipment is available for remote staff. 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 liaisons 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.