COSMOS
Navigate the Compliance Universe

Report on Medicare Compliance Volume 30, Number 9. March 08, 2021

Checklist: Preparing for Downtime Caused by a Cybersecurity Event

By Nina Youngstrom

The Technical Resources, Assistance Center, and Information Exchange in the HHS Office of the Assistant Secretary for Preparedness and Response, better known as ASPR, created this checklist to help organizations prepare for a cyberattack.[1]

HOSPITAL DOWNTIME PREPAREDNESS CHECKLIST

Early preparation and proactive planning for a possible cyber emergency across the hospital or facility will increase effective ***continuity of operations*** and ensure patient safety.

❒ Establish a downtime planning team to oversee preparation efforts, manage ongoing activities, update plans, reinforce training; include IT experts, front-line professionals, hospital operations staff.

❒ Schedule regular processes for reviewing, updating, approving downtime procedures, forms, back-up medical equipment; ensure new/updated forms are compliant, approved by appropriate leads.

❒ Plan for extended downtime disruptions to healthcare operations and patient care (e.g., affected IT systems prompt closing of services). Pre-define criteria for altering services, facility operations.

❒ Establish a "knowledge center" or web-based IC system to store cyber event related information (e.g., status updates, tasks, IT service requests). Ensure staff know how to use the system, understand limitations (e.g., user can only log in as one role though they work at different facilities).

❒ Ensure computers have necessary downtime software and are tested regularly.

❒ Plan for impacted shared drives impacting operations. Consider options for secondary access to critical information (e.g., hospital policies, patient information, employee schedules, on call schedules, staff, and vendor contact information).

❒ Identify secure and convenient area(s) in the hospital to setup paper-based downtime workstations for organizing administrative records, patient charts, and orders. Ensure it is large enough to accommodate several portable workstations and follow facility security requirements.

❒ Develop a comprehensive list of all biomedical equipment, their location, and interdependencies. Have downtime procedures documented for all equipment. If report-back to the EHR is disrupted, have a downtime procedure workflow in place.

Have offline.

❒ Plan a workaround for verifying/documenting health insurance; collecting payment if financial systems are down (e.g., payroll systems, cash payments, procurement cards). Develop downtime ordering and billing workflow instructions (e.g., use of barcodes, hardcopy list of billable supplies, procedure, and process codes).

❒ Inventory older clinical equipment that does not require Internet connectivity or systems access. Assess their condition, document location, and log with other downtime documentation.

❒ Prepare for use of dictation. Create instruction cards for staff unfamiliar with the process and for consistency in dictation style. Maintain a cache of handheld devices, decide who will control them; identify where to submit devices for transcription.

❒ Have color coded paper on-hand to easily identify STAT lab orders, and to prevent non-critical orders from being submitted as high-priority due to lab backlogs during downtime.

❒ Publish and regularly update a repository of nursing station, office, pneumatic tube station numbers.

❒ Ensure adequate supplies of folders, binders, hole punchers, labels for paper charts; avoid having to prepare/procure items during an emergency. Have thumb drives and/or CDs needed to create files.

❒ Be prepared to move copiers/scanners. Map their location/capacity (numbers, color/non color). Ensure adequate paper and toner supplies. Have printing instructions available at workstations for printing medical orders and other information not normally in "printable" format (i.e., how to take a screenshot, reformat documents for print, send jobs to proper printer).