

Date: May 10, 2024
To: All System members
From: Connie J. Mattera, MS, RN, PM
EMS Administrative Director and System Coordinator

System Memo: #431

RE: **URGENT NOTICE: EMS Prep for an Extended Computer Outage**
EMS DOWNTIME PROCEDURES

Cybersecurity threats and actual events are on the rise across all industries - including healthcare. Being prepared to seamlessly deliver care to our citizens during an extended system outage is critical.

We sent a more detailed version of the information below to all System leaders in an email on February 23, 2024. Given the recent Cyber-attack on Alexian Brothers Medical Center this week (see attached memo from Brian Stennett), it is important that we issue key points again.

Please ensure that ALL EMS PERSONNEL are aware of the actions to take in case computer access is disrupted at your agency or within the EMS System.

Send me a return email confirming receipt of this message and that EMS Action Plans are in place.

We encourage all System members to first follow their internal policies. Below are steps to optimize EMS planning, preparedness, and response if computer Systems are disrupted:

EMS DOWNTIME PREPAREDNESS CHECKLIST

- **Plan** for extended downtime disruptions to EMS operations and patient care. Pre-define criteria for altering services and operations to **Crisis capacity (See Policy C3 CRISIS RESPONSE PLAN)**.
- Maintain current paper copies of **Directories** of key EMS personnel (State, Regional Health Departments [See C3 policy], System [EMS MD and Administrative Director]) and their contact information: phone, email, and fax.
- **Ensure paper forms related to EMS care are printed, ready for deployment**, and compliant with EMS standards. If access to the ImageTrend ePCR is disrupted, ensure adequate office supplies are in place to create, store and archive paper PCRs. Have thumb drives readily accessible containing versions of needed EMS documents: **EMS Short PCR Form; Refusal Form; HIPAA Privacy Practices Form**; Patient signature forms; **Bypass Alert forms; Controlled Substance Log**; EMS System Modification forms; etc.
Ensure access to critical EMS standards documents (e.g., **SOPs, policies, procedures**, vendor contact info).
- **Communication is key.** Execute effective workflow communication trees. Ensure that essential stakeholders are notified of your situation and that EMS response and patient care continue to the extent possible within the Crisis response. Identify and attempt to overcome barriers to business continuity.
- **Ensure that MERCI (VHF) radios are checked frequently and are operating effectively.**
- **Ensure that computers have necessary downtime software** and are tested regularly.
- Plan a **workaround for verifying/documenting health insurance; collecting payment** if financial systems are down for an extended time. Develop downtime ordering and billing workflow instructions (e.g., use of barcodes, hardcopy list of billable supplies, procedure, and process codes).
- Inventory older equipment that does not require Internet connectivity or systems access (typewriter etc.). Assess their condition, document location, and log with other downtime documentation.
- Be prepared to move copiers/scanners, printers. Map their location/capacity (numbers, color/non color). Ensure adequate paper and toner supplies. Have printing instructions available at each workstation (How to take a screenshot, reformat documents for print, send jobs to proper printer).

Thank you for supporting our efforts to provide safe care for our patients and community during any type of prolonged downtime or outage. Adapted from: [healthcare-system-cybersecurity-incident-considerations-hospital-downtime-preparedness-checklist.pdf \(hhs.gov\)](https://www.hhs.gov/healthcare-system-cybersecurity-incident-considerations-hospital-downtime-preparedness-checklist.pdf)