Healthcare

ALERTBULLETIN®

A Risk Management Update | 2021 Issue 4

EHR System Outages: Minimizing the Impact of Downtime

Electronic healthcare record (EHR) systems can and do fail. As with all digital networks, they are susceptible to software flaws, malware attacks, hardware failures and interruptions in connectivity, among other problems. (See "Common Sources of EHR System Failure," to the right.)

Such disruptions are more than an inconvenience for aging services organizations. They may endanger resident safety if they impair clinical decision-making, impede access to vital information or distract staff from essential caregiving activities. Moreover, by adversely affecting the delivery, documentation and continuity of care, EHR system outages can potentially lead to liability exposure, regulatory sanctions and reputational damage, as well as problems with billing and other business operations.

When a system failure occurs, the top priority is to maintain critical operations and accurately document ongoing resident care and services. This edition of *AlertBulletin*® is intended to help aging services settings protect residents and mitigate potential losses during an EHR outage by utilizing the following four readiness and response strategies:

- **Prepare for downtime** with a written contingency plan.
- **Promptly communicate the nature and scope of the outage**, as well as the status of recovery efforts, to all stakeholders.
- **Use approved paper documentation formats** during the period of disruption.
- **Synchronize paper records with the EHR** following the outage, in order to preserve a continuous record of care.

Common Sources of EHR System Failure

- **Insufficient encryption capabilities**, resulting in vulnerability to hacking and data theft.
- **Inadequate backup measures** and design redundancy.
- **Mechanical failures** caused by internal hardware problems.
- **Loss of connectivity** due to vendor-host network interruptions.
- **Physical damage to primary data centers** from fire, flood, wind, earthquake, electrical disturbance, or other natural or man-made disaster.
- **Malware** – often linked to "phishing" attacks – that can steal, destroy or distort data, or hold it for ransom.
- **Third-party threats** to "cloud-based" data storage systems.
- **Human error**, exacerbated by ineffective administrative controls, privacy filters or system access safeguards.

Essential takeaway:

The effective management of EHR system outages requires a written contingency plan, data backup, coordinated communication and approved back-up documentation formats.

Preparing for Downtime

The federal HIPAA Security Rule defines aging services organizations as "covered entities." As such, they are required to have a contingency plan and secure data backup system in the event of an EHR outage.

For some facilities, a central element of this backup plan is an internally based Downtime Assessment and Response Team (DART). The team typically consists of IT professionals (either contracted or employed), EHR vendor representatives, nursing and medical directors, unit supervisors, laboratory and pharmacy staff, coordinators for resident admissions and transfers, and other relevant personnel. DARTs can be especially useful in smaller facilities that lack the dedicated onsite IT staff and other crash-recovery resources of larger healthcare institutions.

Aging services DARTs are often assigned the following important outage-related tasks, among others:

Mapping out data flow. By visually depicting the movement of critical data through the organization, leadership can better understand how key systems and applications rely upon and relate to each other. This knowledge, in turn, helps reveal the potential impact of EHR disruption and paper alternatives upon overall facility functioning and specific operations, such as the order-entry system and its decision-support program.

Contingency planning. Contingency plans should address a variety of potential causes of system breakdown and data compromise, including ransomware and other cyber attacks, as well as damage to computers, servers and backup equipment due to floods, fires and acts of vandalism. Once EHR threats are understood, they can be proactively addressed and contained by a combination of redundant system design and effective backup capabilities, such as remote servers and vendor-provided, cloud-based data storage. (To learn more about backup options and their respective advantages and drawbacks, see Adair, B., "Cloud-Based EHR Systems vs. On-Premise," posted on *Selecthub.com*.)

The following risk control strategies can help reduce the risk of data loss or contamination:

- **Prioritize backup of select software applications** used to store, maintain or transmit electronic protected health information (ePHI).
- **Identify all external hard drives used for data backup,** if done locally, and house them in a separate location, whenever feasible.
- **Adopt a "3-2-1" rule when backing up data,** i.e., create *three* copies of data, store them on at least *two* different media and secure *one* copy off-site.
- **Verify the sufficiency of cloud-based backup capability** with the EHR vendor, and rectify any potential deficiencies.
- **Establish clear data restoration procedures,** including how and in what order files will be restored from backup sources, and place a copy of these procedures in a readily accessible location.

Conduct downtime drills. A contingency plan can be effective only if staff know exactly what is expected of them following an EHR outage. By holding quarterly downtime drills across different shifts, workdays and weekends, supervisors can accurately assess staff readiness and ensure that staff members remain conversant with their assigned roles and responsibilities. Help staff members prepare for these drills by developing a training packet that defines individual roles during an outage, including tasks that must be performed manually.

Regularly update outage-related policies and procedures. Following downtime drills, review results and solicit feedback from participants. Apply lessons learned to organizational policies and procedures, in order to ensure that contingency plans remain current, practical and effective.

Communicating Outages

During an outage, the downtime response team is responsible for coordinating communication among administrators, staff, technical personnel, residents and family members. This duty frequently involves crafting a communication plan, establishing a central command center and overseeing the following related tasks, among others:

Maintain a current paper-based contact list. Emergency contact lists are typically stored in electronic form, which may be inaccessible during an outage. As part of their preparedness effort, organizations should print out a paper list of names and contact information and make it readily available for use during a system failure. At a minimum, the list should include administrators, supervisors, staff members, on-call designees, family members, local emergency personnel, vendors and associated outside providers.

Develop an alert system. Once an outage has been identified internally or via an EHR vendor, the first task is to alert affected parties – including staff, medical providers, vendors, residents and families – using such methods as overhead announcements, telephone calls, text messages and emails. The initial alert should answer the following basic questions, among others:

- *What systems are affected?*
- *How serious is the outage?*
- *What is being done to fix the problem?*
- *When is the system expected to be back online?*
- *When is the next planned update?*

Relay frequent updates. Regular bulletins, issued on at least an hourly basis, are essential to minimize chaos and confusion during a disruption. Urgent messages and directives should be relayed in a variety of ways, ranging from staff huddles and leadership rounds to PA announcements, posters, pagers, messaging applications and the facility's website.

Documenting Care Manually

To maintain accurate records during an EHR disruption, facilities must develop and utilize alternative paper documentation formats and procedures that are aligned with current clinical processes and workflows. The following steps, if taken before an outage, can help minimize gaps in the healthcare information record, as well as lapses in clinical communication and delays in care:

Simplify documentation practices. The **SOAP** (**S**ubjective, **O**bjective, **A**ssessment, **P**lan) progress notation system is an established means of creating an effective hard-copy record of care.

Identify vulnerable care operations. When devising alternative, paper-based documentation processes, include safeguards – such as flowsheets, checklists, two-person verifications and handoffs – to help minimize potential problems associated with the following high-risk care situations:

- **Managing clinical emergencies** and behavioral health crises.
- **Arranging transfers** to acute care settings.
- **Capturing advanced directives** regarding healthcare preferences.
- **Verifying medication lists** and drug dosage calculations.
- **Recording allergies** and drug contraindications.
- **Communicating on an urgent basis with practitioners,** e.g., when reporting a resident's rapidly deteriorating condition.
- **Obtaining access to diagnostic images** and laboratory test results.
- **Responding to adverse incidents** and creating a record of investigation and follow-up.
- **Documenting resident/family complaints** and preparing a remedial action plan.

Create paper forms for use during EHR outages. During an unexpected downtime event, the use of pre-approved paper forms helps ensure capture of critical resident care data. The paper equivalent of an electronic resident healthcare information record minimally should include these data categories:

- Resident demographics.
- Medical history, including allergies, illnesses, past procedures and treatments, medications taken and other relevant health information.
- Current pharmacy orders.
- Laboratory tests and results.
- Medical consultations and findings.
- Care plan.
- Advanced directives.
- Case management data.
- External appointment and treatment reports, e.g., dialysis, specialty care.

Pre-approved paper forms should be created with input from relevant staff members, including utilization review and billing personnel, in order to ensure inclusion of key clinical, regulatory and reimbursement-related information. During periodic downtime drills, as well as employee "onboarding" sessions, train staff in proper use of these paper forms, including how to comprehensively document care without benefit of prompting by electronic templates.

Quick Links

- "Patient Safety Guidance for Electronic Health Record Downtime." EHR Downtime Task Force of the Academic Medical Center Patient Safety Organization, 2017.
- Technical Volume 1: "Cybersecurity Practices for Small Health Care Organizations." U.S. Department of Health and Human Services, updated December 28, 2018.
- "Understanding Electronic Health Records, the HIPAA Security Rule, and Cybersecurity." Chapter 4 of the *Guide to Privacy and Security of Electronic Health Information*, version 2.0. Office of the National Coordinator for Health Information Technology, April 2015.

Prepare downtime toolkits. Documentation toolkits should be stored in resident care areas so they are ready for use in the event of an EHR outage. The kits should contain an ample and varied supply of paper forms, including the following, among others:

- Resident labels.
- Admission assessment forms.
- Physician orders.
- Progress notes.
- Nursing care.
- Specialized care notes.
- Vital signs.
- Fluid input/output.
- Medication administration.
- Fall and elopement risk assessments.
- Skin assessment and care.
- Therapy notes.
- Change in condition forms.
- Laboratory and diagnostic requisitions.
- Consultation reports.
- Social work notes.
- Reference materials, including clinical decision-support guides.
- Incident reports.

Synchronizing Paper Records with the EHR

Once the EHR system is restored, the process of entering clinical information can begin. Administrators may opt to designate a data entry team to assist staff members with this potentially time-consuming task. Written synchronization procedures should address the following important considerations:

- **How information will be input,** e.g., manual transcription or scanning of paper documents.
- **How physician orders for medications and treatments will be reconciled,** including for residents who are newly admitted or readmitted following a hospital stay.
- **Whether select documents will remain solely on paper,** such as resident transfer forms, phone messages and routine conveyances.

Handwritten documents should be retained even after they have been entered into the EHR system, as these paper forms and notes constitute the actual record of care during the period of disruption. In addition, the recovery record should indicate the duration of the outage, in order to clarify to data entry personnel which documents need to be transcribed.

Essential takeaway:

Assemble documentation toolkits comprised of essential paper forms for use during an outage and retain handwritten documents even after they are entered into the EHR system.

Occasional computer outages and malfunctions are a fact of life for aging services facilities and other healthcare settings. By establishing secure backup systems, creating and continuously updating contingency and communication plans, and training staff in proper use of paper records, organizations can mitigate disruptions in care and expedite recovery.

Did someone forward this newsletter to you? If you would like to receive future issues of *AlertBulletin*® by email, please register for a complimentary subscription at go.cna.com/HCsubscribe.

For more information, please call us at 866-262-0540 or visit www.cna.com/healthcare.