American Nursing Informatics Association

where Caring & Technology *meet*

Guide and Toolkit

Nursing Downtime Preparedness: From SAFER Guides to Practice

"By failing to prepare, you are preparing to fail."

– Benjamin Franklin

American Nursing Informatics Association
where Caring & Technology meet

Guide and Toolkit

Nursing Downtime Preparedness: From SAFER Guides to Practice

ANIA Downtime Ad Hoc Committee
Elizabeth C. Elkind, PhD, MSN, MBA, RN-BC (Co-Chair)
Denise D. Tyler, DNP, MSN/MBA, RN-BC (Co-Chair)
Karen J. Belotti, MSN, RN-BC
Patricia Berkes, MSN, RN-BC
Lacey Jensen, MN, RN-BC
Jennifer Sheinberg, DNP, RN-BC

Acknowledgments:
Special thanks to our ANIA members and their organizations that shared their downtime documents. Also thanks to Alanna Graham, MSN, RN, for her assistance during the early segment of this project.

ISBN: 978-1-940325-75-0

Nursing Downtime Preparedness: From SAFER Guides to Practice

Nursing downtime preparedness is critical to patient safety. Electronic health records (EHRs) are used in healthcare settings to obtain and review health information, make clinical decisions, and deliver safe and appropriate care (Sano & Alexander, 2019). EHR downtimes can be planned or unplanned. Preparedness is an important goal that supports the proper mechanisms to adequately prepare nurses who are present during a downtime event. Despite processes and policies being in place, many nurses are unfamiliar with them. In some cases, existing policies and procedures are insufficient to properly manage a significant episode of downtime or a prolonged downtime event (Sano & Alexander, 2019). Poor knowledge of these policies and procedures lead to notable reductions in efficiency in patient care, proper management of events, and lack of preparation of the staff (Sano & Alexander, 2019; Schadow et al., 2017). Education and dissemination of policies to staff, especially newly hired nurses, during onboarding proved to be beneficial so that in case of an EHR downtime, they were aware of proper workflows to appropriately continue high quality care and patient safety (Sano & Alexander, 2019).

Organizational policies, according to the Office of the National Coordinator (2014), need to include the following key elements:

- When to call a downtime (recommend calling the downtime within hours of when the system became unavailable).
  - This should include system slowness that prevents a normal workflow.
- How will downtime communication be delivered.
- Who is in charge of the downtime, including technical and operational components.
- How data will be collected during the downtime be entered into the EHR.
- How patients will be registered and identified
- Patient information in read-only systems used for downtime will be secure; generic passwords should be avoided when possible.
- Testing processes (hardware, software, and process/people).
- The location of paper documentation used during the downtime.

The policy must be available in all clinical areas on paper and electronically, and should be reviewed at least every two years. Both staff and leaders need to be involved in this review to ensure it meets the needs of the users and the organization**.** Table 1 reviews key components that should be included in the policy.

Emergency plans need to be in place to ensure healthcare staff can handle downtimes and malfunctions effectively, in addition to analyzing events to prevent errors in continuity of care (Abusalem et al., 2020; Bulson et al., 2017; The Joint Commission, 2022). Preparation is critical to each organization because plans can become quite complex. Needs, such as how to access system downtime reports, how to document on paper forms, and the reconciliation of paper forms, may require in-depth resources. Educational interventions and the provision of appropriate resources have proven to be beneficial in increasing nursing staff's readiness to better manage EHR downtime (Abusalem et al., 2020; Schadow et al., 2017). In-person, hands-on training with downtime manuals helped participants become familiar with protocols, and they were able to review unfamiliar sections (Abusalem et al., 2020). A

Table 1.
Downtime Policy Essential Elements

	Who/What/Where	Summary
Key Stakeholders	• Clinicians • Support staff • Clinical administration Health IT support staff	These members may be part of a downtime committee or a clinical informatics committee that includes end-users. This can be a separate committee, or the duties can be included in the superuser committee.
Who Is Responsible for Activating the System Downtime	The administrator on duty is typically responsible for calling the downtime. Downtime processes should be activated in less than 2 hours of when the system is down.	The administrator on duty (typically the nursing supervisor), after collaboration with the clinical and technical informatics team as well as the administrators on call, will typically announce the downtime. If the situation warrants they will activate the healthcare incident command system.
Policy Location and Availability	A paper copy of the policy should be available for each clinical area in addition to the electronic version.	The policy should be included with the downtime paperwork, whether this is maintained in a binder, a drawer, or a file in each clinical area. A copy should be stored in a safe, off-site location.
Reactivation and Recovery Process	What is entered into the EHR, when, and by whom should be included in the policy. The timeline for entering the information should also be incluuded.	The policy needs to cover who is resposibible for enterig the data obtained during the downtime, along with what is entered. This is especially important for extended downtime events, and for downtime events that cross shifts.
Policy Review	The policy should be reviewed at least every 2 years.	The review should include the superuser or downtime members as well as administration.

simulation viewer also helped staff to demonstrate their ability to access their needed programs to review patient data (Abusalem et al., 2020). Practicing with downtime forms allowed staff to react to scenarios and gain the experience of completing the appropriate paperwork accurately (Abusalem et al., 2020).

Downtime preparedness also includes effective communication methods. Staff must know how to communicate between different disciplines, such as medical, pharmacy, and laboratory (Dave et al., 2020). This also requires transitioning back to paper documentation to perform needed services that would later be integrated back into the EHR, so any harm to patients is avoided (Dave et al., 2020). Staff should know how to send out specimens, access laboratory results, and order radiology procedures to remain safe and efficient. In addition, hands-on training and education, as well as contingency planning, requires teaching staff teamwork to ensure safe and effective management of all hospital information during downtime (Dave et al., 2020). A lack of planning for EHR downtimes allows interruptions in performing nursing tasks completely and safely when systems are down (Roush et al., 2021). It further hinders the nurse's confidence due to the lack of preparedness and knowledge of necessary resources (Roush et al., 2021).

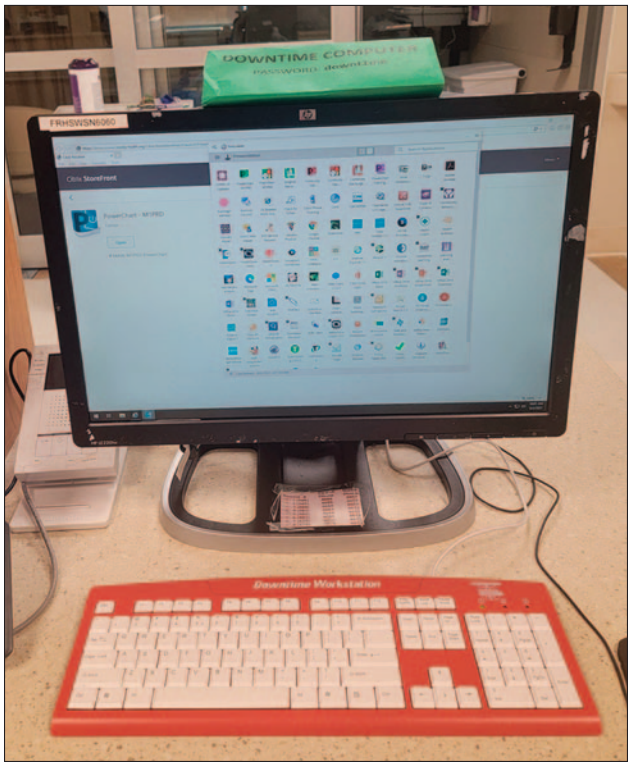
Downtime Standardization

Should Evoke Red Devices

Downtime computers should be clearly labeled. A visual tool can be utilized to label all downtime computers and printers, such as red or red and white-striped tape, to easily identify them during downtimes. Additionally, the computer and red keyboard in Figure 1 quickly and clearly tell staff which workstation is designated and eliminates confusion because they act as a beacon during a hectic situation. Standardization for identifying the downtime computer is important so all staff can be prepared in case of planned, unplanned, or emergency outages (Coffey et al., 2016). Unexpected downtimes of a network or EHR can present risks to patient safety and can even result in the loss of or compromised data (Coffey et al., 2016). Another strategy is the downtime computer having a red and black background with a permanent sign and/or screen saver stating downtime (see Figure 2). These computers should also have lockdown settings that prevent them from turning off to ensure functionality during a downtime event.

The location of computers and downtime protocols should be universally known so the transition during these events are smooth and allow continued function-

Figure 1.
Downtime PC and Keyboard



Used with permission of Denise Tyler.

Figure 2.
Downtime PC Screen

Used with permission from the Children's Hospital of Philadelphia.

ality. This helps nursing staff to function effectively and continue providing safe care. These computers should be in a central location on each unit, such as the nurse's station, and can be used with or without downtimes. It is important they are checked at least weekly, and if something is not working, promptly reported and addressed. The organization should have a method to check daily (an automated utility) that all downtime computers are on the network and able to receive downtime reports. A staff member should assess for accessing and printing reports. If an issue is identified on a downtime computer, then the staff member should submit a ticket to Information Technology (IT). Downtime computers must be plugged in to red emergency outlets (see Figure 3) so they do not go down during a power outage. Depending on the complexity of the systems affected, downtime phones (see Figure 4) may also be required.

Resources

A Nursing Informatics Committee can play a significant role in the governance of downtime. Resources include downtime binders with policy and forms, a hard drive on the computer with policy and key forms, and important phone numbers. The great debate is the downtime binder versus intranet or hard drive access on a computer. Both strategies will work best in case of a ransomware attack, where all electronic devices would need powering down. A downtime box, file drawer, or cart are commonly used to house downtime forms. Downtime policy documents should be short and kept in the downtime binder. These resources should be checked weekly. Downtime forms should be available with sufficient copies, or copies can be made or printed when needed. This may be part of a role for Nursing Informatics Committee members or unit-based Downtime Readiness Champions. A variety of approaches can be used to review and update binders, box file drawers, or whatever is used for storing documents. Figure 5 provides an exemplar of document management for downtime.

Downtime Drills and Assessments

The Centers for Medicare and Medicaid Services (CMS) (2021b), within their Emergency Preparedness appendix, highlights the importance of drills. CMS emphasizes: "Mock disaster drills can also be used to determine if plans can be executed as designed, to assess whether more training is required, or to reinforce best practices" (CMS, 2021b, p. 7). Downtime drills should mimic real patient case scenarios and be enacted with staff on all shifts. Real-life assessment has identified issues where shifts that are accustomed to the downtime will develop workarounds. Previously, downtime drills have been process-focused on nursing clinical tasks, but they should also include practicality and functional aspects. Functionally, nurses should know how to access the downtime policy when the network is up and when it is down. Are users able to find paper forms needed whether from a physical binder or hard drive access?

Figure 3.
Red Outlet

Used with permission of Karen Belotti.

Figure 4.
Downtime Red Phone

Used with permission of Denise Tyler.

Downtime drills should include where downtime computers are and where they should be plugged in. Do computers have access to print all needed reports regardless of location to counteract other issues that can occur unit to unit, such as printers being offline?

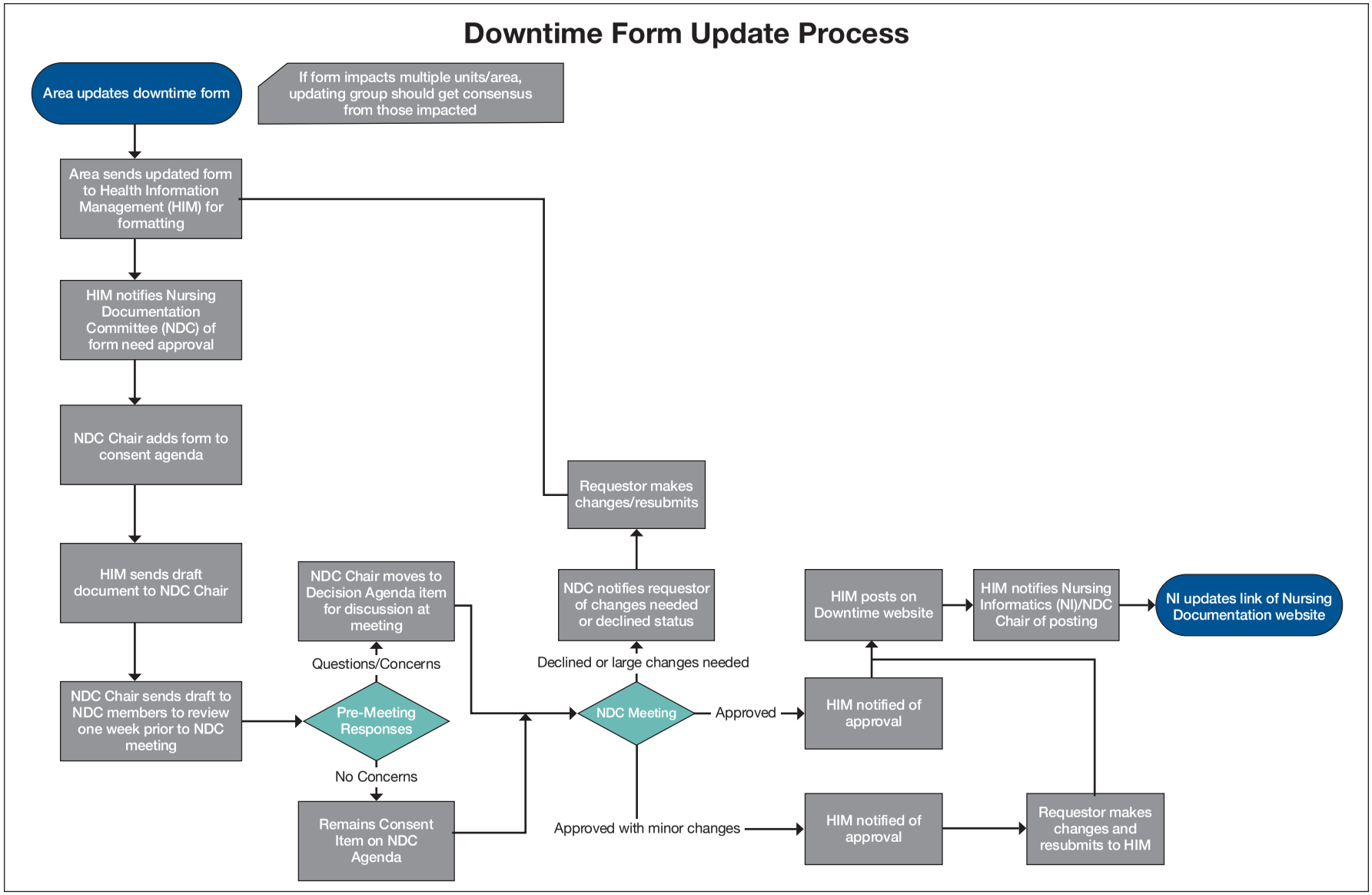
A variety of tools can be used, such as Mock Downtime Drills and assessments (self-assessment and/or peer-assessment). Simulation can also play a part using tabletop exercises for downtime scenarios that can significantly improve the nurse's confidence and ability to perform, and to continue the business plan (Roush et al., 2021). Appendix A provides a drill tool that can be easily transferred into an electronic format such as a Microsoft™ Form or an online survey mode. To further facilitate retrieval of a Microsoft Form, a QR code can be created, and nursing staff can scan it to access the tool. These formats provide electronic data capture to facilitate analysis.

Strategies for sustainability in updating downtime policies and performing downtime drills require healthcare organizations to use a lesson-learned approach to identify, review, and communicate concerns with intent of improving it for the future (Coffey et al., 2016). Ideally, with any new protocol change or update, the informatics nurse may initiate or lead the project, but over time, a collaborative approach is required where nurse managers, informatics committees, EHR super users, and informatics/IT champions can assist with checking resources and running drills (American Nurses Association [ANA], 2015; Sheinberg & Adams, 2021). Recommendations for downtime drills or assessments can vary from unit to unit or organization, but they should be monthly across all shifts until a high comfort level is achieved by users and then modified to quarterly.

Annual Competency

Downtime education, including downtime drills and annual competency, is recommended for all system users. Downtime education should be covered on the unit rather than during onboarding to prevent overload (Golay et al., 2021). This should include a review of the policy and processes, as well as hands-on exercises. This can be done during an in-person performance skills validation, a unit-based in-person validation, and/or using a computer-based training module to simulate how to manipulate online tools. This approach demonstrates individual competency rather than a group problem-solving test. The exercise can include how to print required documents and how to view results. This can be updated as needed to include new policies, processes, equipment, and applications. Updates can also address areas that need to be reviewed based on feedback after system downtimes. Documentation is an essential component of nursing practice, including during downtime (ANA, 2021). Education and competency validation should include the process for

Figure 5.
Document Management for Downtime Exemplar



Used with permission from University of Michigan Medical Center

recovery and reconciliation after the system is available. This is included in the SAFER Guides validation for the promoting operability program (formerly known as meaningful use) (Sittig et al., 2014)

Making the Case for Downtime Drills

A large teaching hospital in central California experienced an 8-hour network downtime on weekend dayshift. The downtime included the desktop and wireless phones because they were voice over internet protocol (VoIP). An added complication was that providers could access the EHR remotely, and the option of adding a notice when signing on to the system was controlled locally, so it was not an option. An internal disaster was called, and a command center was set up. Technical and clinical informatics staff were called in to assist.

The units each had a downtime computer, downtime binders, and a red downtime phone. The downtime computers were clearly marked with a red and white keyboard, and the green downtime binders were organized. Unplanned downtimes were rare, and planned downtimes were always scheduled at night. In addition, weekend staffing often included newer or relief charge nurses

The red analog phones had been set up on each unit when the VoIP had been set up, but they have not been used. Those working did not remember they were available, and they were not clearly visible or labeled. Labels have been ordered and will be applied.

Staff experienced with downtimes and post-downtime functions were not available on each unit. However, these steps were clearly documented in the downtime binder, and they were covered at the afternoon bed meeting. The downtime was called overhead a "Code White" at this organization, and a standard text message was sent out to leaders, including charge nurses. The downtime was cleared after 8 hours, and back charting was required per guidelines. However, when the downtime audit was conducted 2 days later, it was discovered that several units did not follow the guidelines for back charting. This required follow up with managers and backloading of their charting. Managers identified the need for validation of downtime competencies due to inexperience with downtime.

Before this event, downtime drills were approved, and the content was almost completely developed. Leadership determined this process needed to be fast-tracked. The pilot started two weeks after the downtime. The drill was created in Microsoft Forms so it could be completed using a phone, and results were automated. After completing two units and reviewing results, questions were modified, and question fields were modified to drop-down menus, when possible, to improve reporting. The paper form utilized for the post-downtime recovery checklist was also converted to Microsoft Forms. The form did not include "pass or fail" terminology. Instead, the measurement was *Independent, Coached,* or *Complete Assist*. The original paper form included the auditor and the date and time. When the form was moved to an electronic format, these fields were no longer required. The units were built in a drop-down to improve the ability to report on the location, with an "other field" provided in case the unit was not on the list. The drill includes locating downtime resources, such as the binder, the computer, and the phone, as well as finding information and printing documents from the downtime computer.

Downtime Definitions

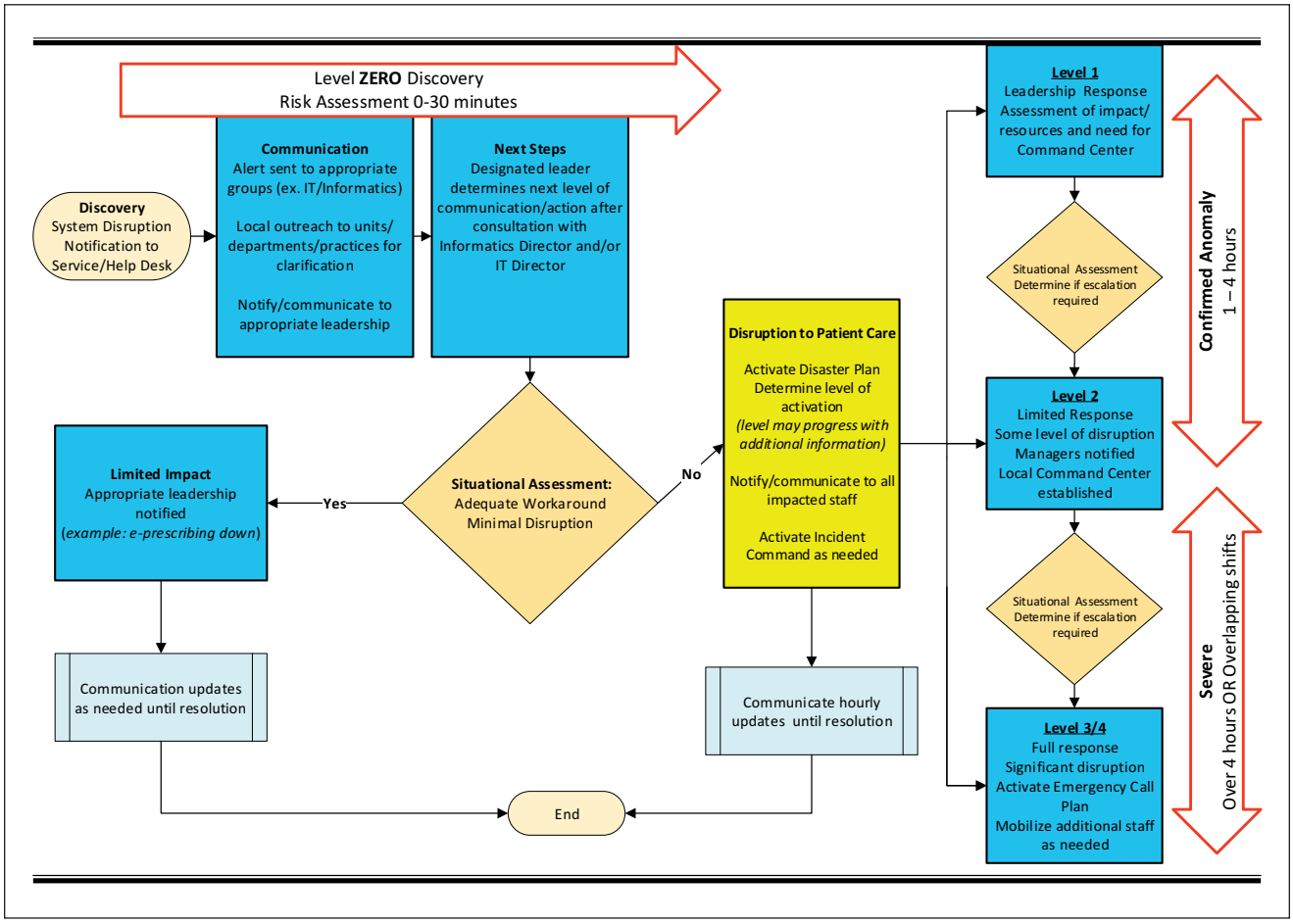
Your organization policy should delineate downtime types. Downtime definitions may vary among organizations. Generally, a **planned downtime** is any period during which the system is fully or partially unavailable (Larsen et al., 2019). These planned periods are operationally disruptive and pose risks to patients, but organizations can mitigate the risk with adequate preparation (Berkes, 2015; Bulson et al., 2017; Schadow et al., 2017). An **unplanned downtime** is any unexpected event where a technology system is unavailable or fails to perform as designed (Massachusetts General Hospital, Center for Disaster Medicine, 2018).

Disaster Definitions and Response

A disaster is any situation that overwhelms available resources. It may be an internal or external event that is static or dynamic. Disaster planning is an essential component of any organization's Emergency Preparedness Program. According to CMS (2021b), an Emergency Preparedness Program is described as "a facility's comprehensive approach to meeting the health, safety and security needs of the facility, its staff, their patient population and community prior to, during and after an emergency or disaster" (p. 7). There are four core elements involved: mitigation, preparedness, response, and recovery (CMS, 2021b; The Joint Commission, 2022). The Joint Commission (2022) includes Cyber/Information Technology as human-caused hazards that present threats, vulnerabilities, and consequences as risks. Hence, risks assessments should be centered around identified hazards followed with training and testing.

Not all downtimes are created equal, and they need to be assessed for severity and impact. The goal is to activate the right resources at the appropriate time for the optimal response. To create an effective plan, different levels of activation determine the response level as outlined below.

Figure 6.
System Interruption Emergency Response



Levels of Activation

- Level 1 Response – Local leadership assesses impact and determines resource needs and next steps levels.
- Level 2 Response – Limited response with Full Incident Command.
- Level 3 Response – Full response with Full Incident Command.
- Level 4 response - Requires Full Incident Command Activation.

Downtime should fall within organizational disaster or emergency preparedness committees for business continuity (Bulson et al., 2017). No matter what committee it falls under, organizations should have established guidelines to work with Emergency Preparedness to determine the appropriate level of response needed (Bulson et al., 2017). The Administrator On-Call, Nursing Supervisor, and other roles as identified by your organization will assess the situation and determine needs and the Level of Disaster Activation. The System Interruption Emergency Response is an example of a process map to determine response levels (see Figure 6).

Communication

Communication plays a crucial role in planned and unplanned downtime events (Academic Medical Center Patient Safety Organization [AMC PSO], 2017; Larsen et al., 2019; Massachusetts General Hospital, Center for Disaster Medicine, 2018). Planned downtimes include pre-downtime communications, which prepare staff for the event. However, an unplanned downtime event does not have the luxury of preplanning. Nonetheless, timely activation and communication of it are emphasized for unplanned events. A standard for communication of the downtime, including type and severity, should be developed and tested, including communication of an “all clear” when the downtime is resolved. This communication may include an overhead announcement, email, text messages, or any combination of the above. Table 2 displays a checklist, which is a useful tool for the informatics team to use to guide the timing of communication and make sure no steps

Table 2.
Planned Downtime Communication Checklist – Exemplars

Task	Time (When Possible)	Completed On/By
Discuss at downtime committee	If possible	
Create downtime flyer(s)	2 weeks before downtime	
Review downtime flyer with informatics team or downtime committee	2 weeks before downtime	
Review at bed meetings/huddles	Daily starting Monday before the downtime	
Review at daily safety huddles	Daily starting Monday before the downtime	
Check printers and fax machines for paper and ink	2 days before the downtime (and weekly)	
Review Downtime binders on units	2 weeks before the downtime (and quarter)	
Verify network downtime process is working and data are available	2 days before the downtime (and weekly)	
Distribute flyers at daily huddles	2 days before the downtime	
Place flyers in common areas	2 days before the downtime	

are missed (Tyler, 2018). Throughout the downtime, communication continues with regular status updates and preparation as the system is getting ready for full function (AMC PSO, 2017; Massachusetts General Hospital, Center for Disaster Medicine, 2018). An exemplar of a flyer that can be customized for the event is found in Appendix B.

Structuring communications with standardized preformatted emails, texts, and phone messages are approaches that facilitate the process and decrease confusion among staff. Email messages may include additional information, such as the current status, the impact, and instructions. Pre-formatted notifications can also include color coding to highlight the type (see Table 3). Texts will be more succinct, so they will require additional instructions via email or flyer (if planned) and documented in an accessible location (see Appendices C and D). When downtimes are part of the disaster planning, the communication may include the type and level of the event.

Table 4 provides an overview of key downtime communications. Appendix C provides exemplars of communication that can be sent via text messages. By pre-populating the messages, the content is standard and clear. A message to telecommunications can be short (for example, "Send out message 1"). Appendix D provides a form that can be filled out for this communication. These messages can be adapted for both planned and unplanned downtime events. Using a standard format and a prepared message guarantees clear and consistent communication.

Table 3.
Notification Color Coding

Planned –	**Blue**
Unplanned –	**Red**
Event (incident) –	**Update**
Event (incident) –	**Resolution**

Ransomware

A ransomware attack is when an organization or user's computer is damaged, disabled, and/or is prevented from use unless a payment is made (Singh & Sittig, 2016). This often leaves users with the options of trying to restore their data from a back-up, paying the ransom, or losing their data altogether (HHS Cybersecurity Program, Office of Information Security, 2021a; Singh & Sittig, 2016). To safeguard against ransomware attacks, health IT must ensure adequate system protection by correctly installing and configuring computers and networks that connect to them (Singh & Sittig, 2016). Reliable system defenses are required by implementing user focused strategies, including simulation and training on correct and complete use of computers and network applications (Singh & Sittig, 2016).

Healthcare organizations need to monitor computer and applications use continuously in an effort to detect suspicious activities to identify and address security problems before they cause harm (HHS Cybersecurity Program, Office of Information Security, 2021a; Singh & Sittig, 2016). Recommendations to prepare for a ransomware attack and increase security include restricting users' ability to install and run software applications, blocking users' access to personal email accounts, monitoring network activity to identify sus-

Table 4.
Downtime Communication – Exemplar

When to Send	Message	Application (s)	Sent Via
Stat	The Clinical System is Down – refer to downtime binders	System outage (EHR)	Email/Text
Stat	Code White	Unplanned system outage (EHR)	Overhead
Planned (scheduled)	The Clinical system downtime preparation – place all new orders on paper and finish charting	System outage (EHR)	Email/Text
	The clinical system is fully available	Downtime resolved (EHR)	Email/Text
	The clinical system is fully available	Downtime resolved (EHR)	Email/Text
	The registration system is down	All registration functions	Email/Text
	The registration system is available	All registration functions	Email/Text
	The Lab (or other ancillary system) is down	Lab, Radiology, Pharmacy, etc.	Email/Text
	The interfaces are caught up	Any interfaces	Email/Text
	The medication dispensing stations are on critical override	Any or all medication dispensing stations are on critical override	Email/Text

picious events, and addressing any deficiencies identified from prior security incidents (Singh & Sittig, 2016).

Cyberattacks are increasingly targeting technology businesses, universities, and hospitals (Poulsen et al., 2020). For example, the SolarWinds hack in 2020, which remains under investigation, has further prompted the need for strategic planning (Poulsen et al., 2020; Temple-Raston, 2021). The HHS Cybersecurity Program, Office of Information Security (2021a) provided a retrospective 2020 review for healthcare cybersecurity. The Health Information Sharing and Analysis Center (H-ISAC) and American Hospital Association (AHA) (2021) collaborated to provide strategic and technical recommendations for hospitals and healthcare systems to prepare and defend future threats. Over one-third of healthcare organizations were impacted by some form of ransomware in 2020 (HHS Cybersecurity Program, Office of Information Security, 2021b). An actual case is provided to underscore the threat and the importance of downtime preparedness.

Case Study

Behavioral Health System is a free-standing behavioral hospital, which is jointly owned by United Health System (UHS) and a local community hospital with a clinically linked EHR. In September 2021, a nationwide ransomware attack struck 400 UHS sites, resulting in $67 million losses in operating income and expenses (Davis, 2021). The ransomware attack affected multiple computer systems, servers, and communication platforms throughout the company, many of which were shut down to contain the breach. To protect the community hospital, communication and EHR interfaces were quickly severed with UHS. Information technology and operations at both sites had to work quickly together to ensure patient safety and minimize disruption to patient care.

The attack affected systems running critical software, applications, and communication platforms, and required a prolonged shutdown (Davis, 2021). Because of the extent of the attack, the EHR was down for 32 days. Traditional servers, computers, and programs utilized for primary EHR downtime were also affected and could not be accessed. Both organizations worked cooperatively to identify and communicate physical downtime forms that could be used as a bridge until the systems could be brought back on-line. When the EHR was recovered, and reconciliation of the paper record was required, leadership decided to recover only active orders and medications using a dedicated recovery team (Davis, 2021). The recovery team consisted of nurses, pharmacists, and a provider with management overseeing the process. Once the EHR was fully recovered, staff documented a full head-to-toe assessment, as well as a recovery note. Recovery time for all admitted patients (62 patients) took approximately 5.5 hours.

Downtime from Start to Post-Reconciliation and Review

Part of downtime preparation includes the steps required when the system is not available in order to maintain a complete and accurate medical record. Policies should include when to initiate downtime charting and

what needs to be backloaded when the system is available (see Appendix E). An example is 2 hours or over a shift change. Integrated devices (e.g., infusion pumps, vital signs, and ventilators) need to be verified before the values are uploaded into the EHR post-downtime. The policy should also include who is responsible for documenting, including documenting by proxy if the staff member who performed the assessment or treatment is unavailable. To decrease the documentation burden, many organizations require backloading only essential clinical information. All paper documentation done during the downtime should be done on approved forms and scanned into the EHR. The organizational policy will also need to encompass whether all paper documentation is scanned into the medical record.

Downtime forms for orders should be specific for each department and include the required components. Frequently used order sets should be available for use during downtime. Include examples of how paper requisition forms should be completed because clinical staff generally either had limited or no experience with it. Orders received during the downtime should be back-entered, and the paper should be scanned into the EHR. Policies or procedures should include follow up on charging.

Recommended Downtime Guidelines

- Planned downtimes should occur when there are generally fewer new orders placed and overall, less activity in the system.
- Due to device integration of vital signs monitors, planned downtimes should start at 15 minutes past the hour.

The process of reconciliation and recovery after a system outage is critical for the ongoing care of each patient and the completeness of the medical record. The EHR downtime and reactivation policies and procedures must be available, complete, and reviewed on a regular basis. This process is part of the annual review of SAFER Guides.

Reconciliation

- To decrease risk to patient safety, after an EHR Downtime, paper documentation needs to be reconciled with the EHR as soon as possible (see Appendix F).
- The length of the downtime impacts the amount of documentation that needs to be reconciled.
- The number of staff required to complete the reconciliation should be directly related to the length of the downtime. Appendix G provides a planning guide.
- If a shift change has not occurred, staff on duty can reconcile documentation, and paper records do not need to be kept and scanned into the EHR.
- If a shift change has occurred, reconciliation staff may update the EHR document, but paper records should be kept and scanned into the EHR for reference.
- Whenever possible, bedside staff should complete the reconciliation of the downtime paper documentation and EHR, if possible.
- In cases of an extended downtime, separate Recovery/Reconciliation teams should be considered for reconciliation as bedside staff care for patients.
- Recovery/Reconciliation Teams are composed of staff who have similar skill sets/clinical experiences and licensure to perform proxy tasks.
- Medication orders during downtime – Pharmacy should have a process to reconcile paper and electronic orders to minimize the risk of duplicate or missed administration.
- Organizations should enter some documentation that serves to communicate a downtime has occurred to alert chart reviewers that paper documents may be scanned into the EHR.

Quality Improvement Process

A variety of terminologies is used for the post-event review (e.g., Hotwash, After Action Review, Post-Event Critical Review, Critical Incident Debrief, and Incident Post-Mortem), and regardless of the terminology chosen, the review and discussion of the downtime event identify problems and patient safety risks. Informatics nurses need to ensure evaluation and reflection of the event (Beausoleil, 2022; Nicol & Dosser, 2016). Reflection provides a strategy to learn through the event and make informed decisions for future downtime planning (Beausoleil, 2022; Nicol & Dosser, 2016).

Surveys can be used to gather satisfaction ratings along with a few open-ended questions of any issues encountered during the downtime event. Simple online surveys can be used to provide feedback before a post-downtime huddle, or debrief. These should be completed within three days, if possible, while the experience is fresh (see Appendix H). This is in keeping with a safety and quality framework, which identifies areas for improvement. A tool can be tweaked according to the specific audience and type of downtime (planned, unplanned, and upgrade), which results in a variety of versions.

The Post-Event Review provides the opportunity to utilize the quality improvement process for improving downtime preparedness. This can be expanded across the healthcare delivery team with modification of the tools. Additionally, CMS released the Final Rule for 2022's Medicare Hospital Inpatient Prospective Payment System, which updates their payment policy and rates. For Fiscal Year 2022, CMS requires hospitals' ac-

tion to it (CMS, 2021a; Sittig et al., 2022). However, the expansion of the CMS rule has significant room for growth in the future, with shared responsibility with EHR vendors and customers (Sittig et al., 2022; Terry, 2021).

Downtime and Post-Event Review has a much bigger impact, and the bottom line is patient safety. At any given moment, nursing is the discipline with the greatest presence at the bedside when our systems fail. We have a professional obligation to know how to continue to care for our patients when technology is unavailable. Being prepared is critical to facing what lies ahead.

References

Abusalem, S., Baer, H., Bates, K., & Crawford, T. (2020). Interventions to improve nurses' response to electronic health record downtimes. *Journal of Informatics Nursing*, *5*(2), 24-28.

Academic Medical Center Patient Safety Organization (AMC PSO). (2017). *Patient safety guidance for electronic health record downtime.* https://rmf.harvard.edu/Clinician-Resources/Guidelines-Algorithms/2017/EHR-Downtime-Guidelines

American Nurses Association (ANA). (2015). *Nursing informatics: Scope and standards of practice* (2nd ed.). Author.

American Nurses Association (ANA). (2021). *Nursing: Scope and standards of practice* (4th ed.). Author.

Beausoleil, A.M. (2022) Reflective practice and design. In: *Business design thinking and doing* (pp. 117-133). Palgrave Macmillan. https://doi.org/10.1007/978-3-030-86489-7_7

Berkes, P. (2015, April 23). *Computer system downtime: What "building blocks" need to be in place for patient safety.* Pre-conference session presented at the 2015 ANIA Annual Conference, Philadelphia, PA.

Bulson, J., Van Dyke, M., & Skibinski, N. (2017). Rebooting healthcare information technology downtime management. *Journal of Business Continuity & Emergency Planning, 11*(1), 63-72.

Centers for Medicare & Medicaid Services (CMS). (2021a). *Fact sheet: Fiscal year (FY) 2022 Medicare hospital inpatient prospective payment system (IPPS) and long term care hospital (LTCH) rates final rule (CMS-1752-F).* https://www.cms.gov/newsroom/fact-sheets/fiscal-year-fy-2022-medicare-hospital-inpatient-prospective-payment-system-ipps-and-long-term-care-0

Centers for Medicare & Medicaid Services (CMS). (2021b). *State operations manual: Appendix Z – Emergency preparedness for all provider and certified supplier types interpretive guidance.* https://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Downloads/som107ap_z_emergprep.pdf

Coffey, P.S., Postal, S., Houston, S.M., & McKeeby, J.W. (2016). Lessons learned from an electronic health record downtime. *Perspectives*. https://library.ahima.org/doc?oid=301846#.YnW1OoXMKUk

Dave, K., Boorman, R.J., & Walker, R.M. (2020). Management of a critical downtime event involving integrated electronic health record. *Collegian*, *27*(5), 542-552. https://doi.org/10.1016/j.colegn.2020.02.002

Davis, J. (2021). UHS ransomware attack cost $67M in lost revenue, recovery efforts. *Health IT Security*. https://healthitsecurity.com/news/uhs-ransomware-attack-cost-67-million-in-recovery-lost-revenue

Golay, D., Salminen Karlsson, M., & Cajander, Å. (2021). Negative emotions induced by work-related information technology use in hospital nursing. *Computers, Informatics, Nursing*, *40*(2), 113-120. https://doi.org/10.1097/CIN.0000000000000800

Health Information Sharing and Analysis Center (H-ISAC) & American Hospital Association (AHA). (2021). *Strategic threat intelligence: Preparing for the next "SolarWinds" event* [white paper]. https://www.aha.org/system/files/media/file/2021/04/hisac-aha-white-paper-strategic-threat-intelligence-preparing-for-next-solarwinds-event.pdf

HHS Cybersecurity Program, Office of Information Security. (2021a). *2020: A retrospective look at healthcare cybersecurity.* https://www.hhs.gov/sites/default/files/2020-hph-cybersecurty-retrospective-tlpwhite.pdf

HHS Cybersecurity Program, Office of Information Security. (2021b). *Ransomware trends 2021.* https://www.aha.org/system/files/media/file/2021/06/hc3-tlp-white-threat-intelligence-briefing-ransomware-trends-2021-6-3-21.pdf

Larsen, E., Hoffman, D., Rivera, C., Kleiner, B.M., Wernz, C., & Ratwani, R.M. (2019). Continuing patient care during electronic health record downtime. *Applied Clinical Informatics*, *10*(3), 495-504. https://doi.org/10.1055/s-0039-1692678

Massachusetts General Hospital, Center for Disaster Medicine. (2018). *Hospital preparedness for unplanned information technology downtime events: A toolkit for planning and response.* https://www.massgeneral.org/assets/MGH/pdf/emergency-medicine/Downtime-Toolkit.pdf

Nicol, J.S., & Dosser, I. (2016). Understanding reflective practice. *Nursing Standard, 30* (6), 34-40.

Office of the National Coordinator. (2014). *General instructions for the SAFER self-assessment guides.* https://www.healthit.gov/sites/default/files/safer/pdfs/safer_highprioritypractices_sg001_form_0.pdf

Poulsen, K., McMillian, R., & Volz, D. (2020, Dec. 21). SolarWinds hack victims: From tech companies to a hospital and university. *Wall Street Journal.* https://www.wsj.com/articles/solarwinds-hack-victims-from-tech-companies-to-a-hospital-and-university-11608548402

Roush, K., Opsahl, A., Parker, K., & Davis, J. (2021). Business continuity planning: *Nurse Leader*. https://doi.org/10.1016/j.mnl.2021.01.003

Sano, J.M., & Alexander, S. (2019). Using an evidence-based approach for electronic health record downtime education in nurse onboarding. *Computers, Informatics, Nursing*, *38*(1), 36-44. https://doi.org/10.1097/cin.0000000000000582

Schadow, M.B., Belotti, K., & Lackart, K. (2017, March 31). *Fixin' to jazz up downtime: The effects of serial mock computer downtime drills on IOS nurses' perceived knowledge of downtime response.* Podium session presented at the 2017 ANIA Annual Conference, New Orleans, LA.

Sheinberg, J., & Adams, V. (2021, August 4). *All aboard: Redesigning procedural drill to navigate successful downtime engagement.* Podium session presented at the 2021 ANIA Annual Conference, San Diego, CA.

Singh, H., & Sittig, D. (2016). A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks. *Applied Clinical Informatics*, *7*(02), 624-632. https://doi.org/10.4338/aci-2016-04-soa-0064

Sittig, D.F., Ash, J., & Singh, H. (2014). *SAFER guides: Safety assurance factors for EHR resilience.* https://www.healthit.gov/topic/safety/safer-guides

Sittig, D.F., Sengstack, P., & Singh, H. (2022). Guidelines for US hospitals and clinicians on assessment of electronic health record safety using SAFER Guides. *JAMA*, E1-E2._https://doi.org/10.1001/jama.2022.0085

Temple-Raston, D. (2021, April 29). *Biden order to require new cybersecurity standards in response to SolarWinds attack.* https://www.npr.org/2021/04/29/991333036/biden-order-to-require-new-cybersecurity-standards-in-response-to-solarwinds-att

Terry, K. (2021, September 14). New CMS rule challenges hospitals, but not vendors, to make EHRs safer. *The Hospitalist.* https://www.the-hospitalist.org/hospitalist/article/246089/business-medicine/new-cms-rule-challenges-hospitals-not-vendors-make-ehrs

The Joint Commission. (2022). *Emergency management.* https://www.jointcommission.org/resources/patient-safety-topics/emergency-management/

Tyler, D. (2018). A day in the life of an informatics nurse: Downtime – Beyond academics. *Journal of Informatics Nursing, 3*(4) 16-18.

American Nursing Informatics Association

where Caring & Technology *meet*

Toolkit
Table of Contents

Note: The American Nursing Informatics Association grants permission to modify and use these tools in your facility.

* Downloadable interactive version available. Look for the and instructions at the top of the first page of the tool.

Appendix A.

Click here for an interactive version of this tool.

Downtime Drill Tool

Mock Computer Downtime Drill Standardized Process and Questions Tool

Adapted from Schadow et al. (2017)

1. Unit (required response from Drop Down):
   Select your answer.

2. Unit (if not in Drop Down): _____

3. Staff member last name: _____

4. Staff member first name: _____

5. Number of years employed: _____

6. Has the staff member done this drill before?
   - ☐ Yes
   - ☐ No

7. If yes, provide an approximate number of times? _____

8. Please show me where your material is located.
   - ☐ Independent
   - ☐ Coached
   - ☐ Complete Assist

9. Please find a requisition for a lab order.
   - ☐ Independent
   - ☐ Coached
   - ☐ Complete Assist

10. You receive a new admission during downtime. Show me what paper forms you will use to document admission data.
    - ☐ Independent
    - ☐ Coached
    - ☐ Complete Assist

11. During the downtime, there is an order to obtain a routine urinalysis on one of your patients. Please describe how the specimen will get labelled and sent to the lab.
    - ☐ Independent
    - ☐ Coached
    - ☐ Complete Assist

12. Please take me to your downtime computer.
    - ☐ Independent
    - ☐ Coached
    - ☐ Complete Assist

13. Verify that you have an adequate supply of printer supplies (for example, paper, toner, labels) for a downtime.
    - ☐ Independent
    - ☐ Coached
    - ☐ Complete Assist

14. Please sign in to your downtime computer.
    - ☐ Independent
    - ☐ Coached
    - ☐ Complete Assist

15. Please demonstrate how you would print a downtime medication administration record (MAR) for one of your patients.
    - ☐ Independent
    - ☐ Coached
    - ☐ Complete Assist

16. Please demonstrate how you would print your unit census.
    - ☐ Independent
    - ☐ Coached
    - ☐ Complete Assist

17. Demonstrate how you would find a lab order or a lab result before the computers went down.
    - ☐ Independent
    - ☐ Coached
    - ☐ Complete Assist

18. Show me where would you find written orders entered on the patient during the downtime.
    - ☐ Independent
    - ☐ Coached
    - ☐ Complete Assist

19. There is a complete network failure, so all electronically stored downtime forms are inaccessible. Where else can you find these forms?
    - ☐ Independent
    - ☐ Coached
    - ☐ Complete Assist

20. The telephone/wireless network are down. How would you call a code or contact the operator (for example, analog phones, fax machines, and/or walkie-talkies) using your red analog phone?
    - ☐ Independent
    - ☐ Coached
    - ☐ Complete Assist

21. Where would you document in [Insert system name] if the system was down in the EHR, would you document the system was down for 8 hours?
    - ☐ Independent
    - ☐ Coached
    - ☐ Complete Assist

22. Demonstrate how you would access your downtime tracking board (name).
    - ☐ Independent
    - ☐ Coached
    - ☐ Complete Assist
    - ☐ N/A

23. Comments _____

_____

_____

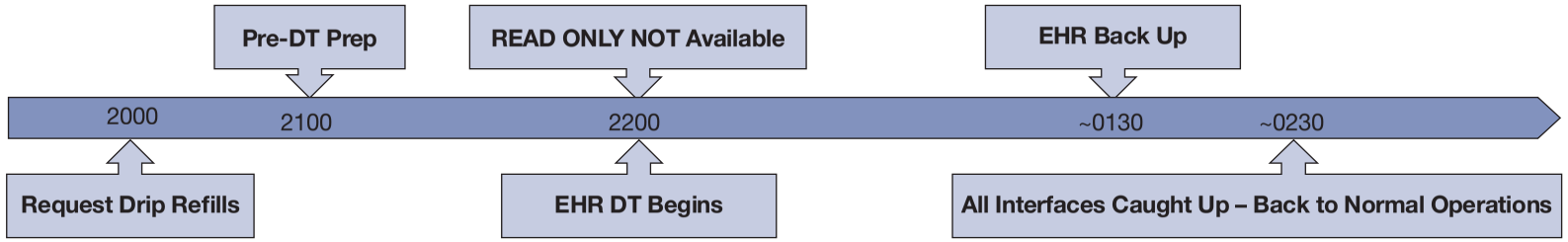
_____

Source:

Schadow, M.B., Belotti, K., & Lackart, K. (2017, March 31). *Fixin' to jazz up downtime: The effects of serial mock computer downtime drills on IOS nurses' perceived knowledge of downtime response.* Podium session presented at the 2017 ANIA Annual Conference, New Orleans, LA.

Appendix B.

Exemplar EHR Downtime Form



Key Points

Patient Registration

- Patient registration will be used.
- Provide 3 sheets of labels for patients starting at 2000 hours.

Lab

- Continue to enter lab orders until 2050.
- Send all labs with downtime requisition form (paper form).
- Send 5 labels for each test (i.e., CBC + Potassium = 10 labels).
- Send STAT draws on a requisition for phlebotomist collection.
- **Include on ALL reqs: Department FAX# and patient room**

Imaging/EKGs

- Paper orders.
- Results available in the DT viewing system online or by Fax/Print received by ED.

Acuity: Not updated during DT.

Staff Assignment System: Not updated during DT.

Bed Tracking: ED – Fax bed requests to bed-control/registrations.

Supply Cabinets: Add "temporary" patients.

Nursing Units

- Print DT forms- Patient Census/MAR from a designated Downtime Computer.
- Print sufficient labels prior to downtime (do not call Registration).
- Each paper form needs a label.
- Use paper requisitions for ALL orders.
- RT orders – Call/page new and STAT orders.
  Call all Transfers/Discharges/Admits to bed control.
- Fax medication orders to Pharmacy.
- Please send medication drip refill requests to pharmacy 2 hours prior to the downtime.
- **Medication Cabinets:** Will be on critical override and new patients will need to be manually entered.
  1. Under patient screen, access "Add Temp Patient" button on bottom right.
  2. Enter patient First Name, Last Name, and FIN into ID.

Verify the correct information when entering new patients

- Use the ***"Override"*** function, in which all meds loaded in Pyxis are available to be overridden during critical override.
- Use the "Remove" function for current medications, this does not work for new med.

Recovery:

1) Anticipate at least 30 minutes for interfaces to catch up.
2) For any issues- please enter ticket x53200 or Service Now.
3) **NO need to enter Significant Event Form** since the clinical EHR is not down.
4) Verify patient location in various applications.
5) Please send any debrief items/learnings to the downtime coordinator.

Note: DT = downtime, ED = emergency department, CBC = complete blood count, RT = recovery team, EHR = eletronic health record

Appendix C.

Sample Text Messages Master Table

Clinical System (EHR)		
Message Number	**Purpose**	**Message Content**
1	EHR disruptions not declared downtime	**Subject:** EHR DISRUPTION **Body:** Use paper processes for urgent needs
2	EHR downtime: Unscheduled or scheduled declared by system office	**Subject:** EHR DOWNTIME **Body:** Follow downtime procedures in [insert – binder, cart, or drawer]
3	EHR downtime Read only availability	**Subject:** EHR READ ONLY AVAILABLE **Body:** Log on to [insert specifics]
4	EHR downtime complete	**Subject:** EHR NOW AVAILABLE **Body:** Start recovery process. Continue using paper orders.
5	EHR disruption complete	**Subject:** EHR FULLY AVAILABLE **Body:** Complete [insert specifics]. Place ALL ORDERS in EHR.
6	EHR downtime preparation	**Subject:** EHR START DOWNTIME PREPARATION **Body:** 30 min before downtime; place ALL NEW ORDERS on paper and finish charting

Lab System		
Message Number	**Purpose**	**Message Content**
7	Lab downtime	**Subject:** LAB DOWNTIME **Body:** Use paper process for urgent needs.
8	Lab availability	**Subject:** LAB NOW AVAILABLE **Body:** Do not backload paper orders in EHR.

Interface Disruption		
Message Number	**Purpose**	**Message Content**
9	XXX interface disruptions when orders, results, ADTs, etc. are not crossing between systems.	**Subject:** XXX INTERFACE DISRUPTION **Body:** Use paper processes for urgent needs

ADT		
Message Number	**Purpose**	**Message Content**
10	ADT downtime	**Subject:** ADT DOWNTIME STARTED **Body:** Use downtime process.
11	ADT availability	**Subject:** ADT DOWNTIME COMPLETE **Body:** System available for use.

Appendix D.

Text Message Request Samples

Sample – Text Message Request #2

Date: _____ Time: _____

Requested by: _____ Phone #: _____

☐ STAT ☐ Within 1 hour ☐ Other

Send text message to: Downtime Communication Group

Subject (limit to 30 digits – including spaces and punctuation)
EHR NOW AVAILABLE

Body of text (limit to 50 digits – including spaces and punctuation)
Follow downtime procedures in XXXX binder

Send form to PBX Operator at XXXX and call "0" to alert them it is coming.

Completed by: _____ _____
Operator Time

Sample – Text Message Request #4

Date: _____ Time: _____

Requested by: _____ Phone #: _____

☐ STAT ☐ Within 1 hour ☐ Other

Send text message to: Downtime Communication Group

Subject (limit to 30 digits – including spaces and punctuation)
EHR NOW AVAILABLE

Body of text (limit to 50 digits – including spaces and punctuation)
Start recovery process. Place STAT orders on paper.

Send form to PBX Operator at XXXX and call "0" to alert them it is coming.

Completed by: _____ _____
Operator Time

Sample – Text Message Request #7

Date: _____ Time: _____

Requested by: _____ Phone #: _____

☐ STAT ☐ Within 1 hour ☐ Other

Send text message to: Downtime Communication Group

Subject (limit to 30 digits – including spaces and punctuation)
LAB DOWNTIME

Body of text (limit to 50 digits – including spaces and punctuation)
Use paper processes for urgent needs.

Send form to PBX Operator at XXXX and call "0" to alert them it is coming.

Completed by: _____ _____
Operator Time

Sample – Text Message Request #8

Date: _____ Time: _____

Requested by: _____ Phone #: _____

☐ STAT ☐ Within 1 hour ☐ Other

Send text message to: Downtime Communication Group

Subject (limit to 30 digits – including spaces and punctuation)
LAB NOW AVAILABLE

Body of text (limit to 50 digits – including spaces and punctuation)
DO NOT backload STAT Lab/Rad paper orders already faxed or tubed.

Send form to PBX Operator at XXXX and call "0" to alert them it is coming.

Completed by: _____ _____
Operator Time

Appendix E.

Downtime and Recovery Charting

Part of downtime preparation includes the steps required when the system is available in order to maintain a complete and accurate medical record. To decrease the documentation burden, many organizations require back-loading only essential clinical information. All paper documentation should be done on approved forms and scanned into the electronic health record (EHR). The organizational policy will need to encompass whether all paper documentation is scanned into the medical record. Policies should also include when to start documenting on paper, what to backload, and guidelines for documenting by proxy in case the downtime crosses shifts. For example, after the system has been down for 2 hours or more, all documentation completed on paper will be scanned into the record. If the downtime crosses a shift change, charting by proxy will be implemented.

Downtime forms for orders should be specific for each department and include the required components. Frequently used order sets should be available for use during downtime. Orders received during the downtime should be back-entered, and the paper should be scanned into the EHR. Policies or procedures should include follow up on charging.

	Down	Up	
Documentation Type	**Downtime Forms and Resources**	**What to Document When EHR Is Up**	**Reconciliation and Recovery Documentation**
Back entering documentation and scanning paper records into EHR per organization policy	Only paper forms approved by the organization "forms" committee will be used.	If downtime is greater than 2 hours or crosses a shift, specified documents will be back-entered into the EHR.	All paper downtime documentation will be entered on approved forms and scanned into the document imaging system per policy.
New admissions (allergies, pre-admission meds, recent immunizations history, etc.)	Paper downtime form/ flowsheet.	Allergies, home medications, immunizations, history, the admission assessment, and vital signs. Medication administered during the downtime should be back-entered to avoid double dosing.	These components significantly impact medication reconciliation, safe medication administration, and triggers and alerts. They may be documented in the EHR by the team member who performed them or by proxy.
Medication orders	Complete paper order form and send to pharmacy. Use a job aide to identify order requirements (fields). *Include all appropriate patient identifiers, allergies, and weight. **Follow policy for STAT orders.	Orders activity.	The reconciliation team, including the pharmacy, will back-enter orders in EHR. If a staff member who documented on paper is not available during chart reconciliation, the documentation should be entered by proxy. Organizational policy dictates when and what paper documents are scanned into EHR.
Medication administration record (MAR)	EHR downtime MAR report.	Medications administered during the downtime.	Staff should document in EHR once the system is available. If done by proxy, document "given by" and retain the paper form.

continued on next page

Documentation Type	Down	Up	
	Downtime Forms and Resources	**What to Document When EHR Is Up**	**Reconciliation and Recovery Documentation**
Reconciling medications	Reports from medication dispensing machines.	Report from the dispensing machine and the MAR.	Nursing or pharmacy needs to review the medications pulled from the dispensing machine and compare them to the paper MAR, the order, and documentation in the EHR to ensure accuracy. Charges also need to be reconciled.
Lab orders	Complete paper order requisition and send to the lab. Use a job aide to identify order requirements (fields). *Follow policy for STAT orders.	Not applicable.	Lab staff will enter orders completed during the downtime. Nursing will enter future and recurring orders.
Radiology/imaging orders	Complete radiology paper requisition and send to radiology. Use a job aide to identify order requirements.	Ancillary orders activity, tech worklist activity.	Radiology will enter orders completed during the downtime. Nursing will enter recurring orders.
Flowsheet	Paper flowsheet.	Flowsheets.	Back-charting flowsheet data in EHR will be driven by organizational policy. Examples of what should be documented include intake and output, point-of-care testing, restraints, and immunizations.
Vital signs (including height and weight)	Paper flowsheet.	Flowsheets.	Per organizational policy, some data will be entered in EHR manually. Examples include admission data, daily weight, and vitals.
Delivery summary	Paper.	EHR delivery summary and mark as complete.	Staff will document in delivery summary when EHR is back up.
Notes	On paper progress notes.	Notes activity.	This can be scanned into EHR, or users can wait till EHR is up to chart. Keep documentation on approved downtime forms, then back-enter per policy when the system is available.
Plan of care/education	This may be documented on approved forms during downtime.	Plan of care/education activity.	Document in EHR when it is available.

continued on next page

Documentation Type	Down	Up	
	Downtime Forms and Resources	**What to Document When EHR Is Up**	**Reconciliation and Recovery Documentation**
Charges	Paper.	Charge capture.	Departments will be responsible for auditing and manually entering charges per organizational policy.
Communication in chart of downtime	—	—	Documentation in EHR in a standard location the time the system was down. Example: "System down 2/22/22 from 08 to 1800."
Procedural Areas			
Documentation type	Approved paper forms.	Back-enter per organizational policy.	Staff will document based on policy, including a minimum of staff, procedure, and times.
Scheduling cases (surgical and procedural)	Print out the report of scheduled cases and the preference cards. Call scheduler to schedule new cases.	The scheduler will back-enter future cases.	The case may be back-entered per policy. Example: May back-enter procedure, staff, and start/stop times.
Log documentation	Paper documentation will begin prior to scheduled downtime.	All log data will be entered electronically into EHR.	Follow the above policies and correlate areas of log documentation.
Central supply sterile processing	Support departments will have access to preference card information.	—	Back-enter/enter charges per policy.
Anesthesia Vitals	Paper flowsheet.	—	Restart auto-validation if applicable.
Preop, PACU, postop	Paper flowsheet.	—	Back-enter/enter charges per policy.

Appendix F.

Click here for an interactive version of this tool.

Post-Downtime Checklist

1. Unit.
   Select your specific unit from Drop Down.

2. Unit (if not in Drop Down).

3. Verify the census on the unit matches the census in the computer.
   - ☐ Yes
   - ☐ No
   - ☐ NA/Other

4. Verify all patients have the correct wristband on.
   - ☐ Yes
   - ☐ No
   - ☐ NA/Other

5. Verify all patient information has crossed into other applications (OB, Monitors, Pyxis, etc.).
   - ☐ Yes
   - ☐ No
   - ☐ NA/Other

6. Verify all orders received during downtime that are still active (to be done) are back-loaded.
   - ☐ Yes
   - ☐ No
   - ☐ NA/Other

7. Verify all paper documentation completed during downtime are placed in the paper chart.
   - ☐ Yes
   - ☐ No
   - ☐ NA/Other

8. Verify backload documentation in [insert system] is completed (see green downtime binder).
   - ☐ Yes
   - ☐ No
   - ☐ NA/Other

9. Complete Downtime Audit Tool and Significant Event Form for each patient.
   - ☐ Yes
   - ☐ No
   - ☐ NA/Other

10. Any discrepancy found during the audit process will be entered as an incident report in [insert where].
    - ☐ Yes
    - ☐ No
    - ☐ NA/Other

11. Restock the Downtime [binder, cart, or drawer] (forms, requisitions, order sheets, etc.).
    - ☐ Yes
    - ☐ No
    - ☐ NA/Other

12. Comments (follow up, ticket entered, etc.). _____

    _____

    _____

Appendix G.

Click here for an interactive version of this tool.

Exemplar: How to Estimate Hours Backload Will Take

This tool is to help streamline the decision-making and process around the backload of patient orders after a downtime.

Prior to systems coming back up:

1. Determine census on each unit.
    a. Determine how many patients are going home in the immediate shift (or next 12 hours).
        i. Orders for these patients will remain on paper for the remainder of their stay and NOT be back-loaded.
            (1) This typically means there may be a few units that will have NO backload, such as the emergency department and same-day procedure.
    b. For the remaining units:
        i. From number of patients not going home in the immediate shift:
            (1) Determine how many patients were admitted during the downtime (their backload takes longer).

Based on a formula that admissions average 1.5 hours of backload and every remaining patient who is not going home in the immediate shift will have 0.5 hours of backload for every 24 hours of downtime (backload hours for these patients change based on how many hours down).

Sample Backload Estimation Tool

Unit	Census	Going Home	Patients to Backload			# Hours System Down	Estimated Time to Backload
			Remaining (Census – Go Home)	Admit during DT (Breakdown of Backload of Remaining)	Here Prior and After (Breakdown of Backload of Remaining)		
2N						24	0
2S						24	0
3N						24	0
3S						24	0
4N						24	0
4W						24	0
Peds						24	0
NICU						24	0
CVICU						24	0
ICU						24	0
PCU						24	0
T7						24	0
T8						24	0
Station II						24	0
	0			**0**	**0**		**0**

Backload hours	**0**
How many hours before your backload to be complete	**4**
Number of Backload staff needed:	**0**

Determine goal for orders backload to be complete. Divide backload hours by that number. This gives you the number of estimated backload staff you will need to accomplish the backload by the time you want to come up.

Samples of How It Could Look for 24- and 12-Hour Downtimes

24-Hour Downtime

Unit	Census	Going Home	Patients to Backload			# Hours System Down	Estimated Time to Backload
			Remaining (Census – Go Home)	Admit during DT	Here Prior and After		
				(Breakdown of Backload of Remaining)			
2N	20	10	10	5	5	24	10
2S	20	10	10	5	5	24	10
3N	20	10	10	10	0	24	15
3S	20	10	10	0	10	24	5
4N	20	10	10	4	6	24	9
4W	10	2	8	0	8	24	4
Peds	1	0	1	0	1	24	0.5
NICU	10	1	9	4	5	24	8.5
CVICU	20	10	10	7	3	24	12
ICU	20	10	10	2	8	24	7
PCU	20	10	10	3	7	24	8
T7	20	10	10	5	5	24	10
T8	20	10	10	1	9	24	6
Station II	10	0	10	3	7	24	8
	231			**49**	**79**		**113**

Backload hours	**113**
How many hours before your backload to be complete	**4**
Number of Backload staff needed:	**28.25**

Samples of How It Could Look for 24- and 12-Hour Downtimes

12-Hour Downtime

Unit	Census	Going Home	Patients to Backload			# Hours System Down	Estimated Time to Backload
			Remaining (Census – Go Home)	Admit during DT	Here prior and after		
				(Breakdown of Backload of Remaining)			
2N	36	10	10	3	30	12	12
2S	36	10	10	2	30	12	10.5
3N	36	10	10	6	30	12	16.5
3S	36	10	10	0	30	12	7.5
4N	30	10	10	3	30	12	12
4S	30	2	8	0	30	12	7.5
Peds	6	0	1	5	10	12	10
L&D	30	5	25	5	25	12	13.75
MB	30	5	25	5	25	12	13.75
NICU	10	1	9	2	10	12	5.5
CVICU	25	10	10	5	30	12	15
ICU	20	10	10	5	30	12	15
CCU	25	10	10	5	30	12	15
4T	20	10	10	5	30	12	15
MH	20	10	10	5	36	12	16.5
Rehab	10	0	10	5	30	12	15
	400			**61**	**436**		**200.5**

Backload hours	**200.5**
How many hours before your backload to be complete	**24**
Number of Backload staff needed:	**8.35**

Appendix H.

Click here for an interactive version of this tool.

Post-Downtime Huddle

Questions with ratings are on a scale of 1 to 5 (1 = Not Very Satisfied and 5 = Very Satisfied).

1. Were you present during the downtime? If you were not present, answer the following questions based upon the staff feedback you received.
   ☐ Yes
   ☐ No

2. Rate: How prepared were you for the downtime?
   1 2 3 4 5

3. Rate: How confident did you feel in relaying information to your respective units?
   1 2 3 4 5

4. Rate: Was the communication before downtime adequate to prepare you and your staff?
   1 2 3 4 5

5. Rate: How confident were you or your floor in relaying concerns to the Clinical Command Center during the event?
   1 2 3 4 5

6. Rate: Your overall preparedness in respect to the downtime and reconciliation?
   1 2 3 4 5

7. Did you use any of the supporting documents during the downtime and reconciliation?
   ☐ Yes
   ☐ No

8. If yes, rate how useful were the supporting documents that were used during the downtime and reconciliation.
   1 2 3 4 5

9. Rate: The usefulness of materials for downtime.
   1 2 3 4 5

10. Have you or your unit participated in downtime drills in the last 4 months?
    ☐ Yes
    ☐ No

11. Did you feel that the unit downtime drills were helpful in preparing for a downtime event?
    ☐ Yes
    ☐ No

12. [Free text] If no, what did you not feel prepared for? Please explain.

13. [Free text] How could communication before downtime be improved?

14. [Free text] How could communication during downtime be improved?