JULY 2018

Hospital Preparedness for Unplanned Information Technology Downtime Events

A Toolkit for Planning and Response

MGH 1811
MASSACHUSETTS
GENERAL HOSPITAL
CENTER FOR
DISASTER MEDICINE

CONTENTS

CONTENTS CONTINUED

/// Executive Summary

Since 2008, use of information technology (IT), including electronic health records (EHRs), has increased more than eight-fold in U.S. hospitals.[1] Additionally, healthcare's increasing reliance on IT is not limited to support of direct patient care activities, but commonly now extends to nearly every aspect of daily operations, from supply chain management, nutrition services, finance, and beyond. Yet, while this increasing use of IT offers many benefits, one critical assumption on which these well-documented advantages are based is the uninterrupted operational status of the systems and technologies in use. When IT services fail, unplanned downtime events occur and each of the putative benefits of IT systems (such as improvements in speed and efficiency, integration of information, reduction of errors, and communication), can become an area of major vulnerability for the hospital. Without functioning IT systems, hospital throughput and efficiency immediately decline, communication is challenged, and carefully designed safety systems are often unavailable.

In many cases hospitals' abilities to manage their unplanned IT downtime events have substantially lagged behind their adoption of new technologies. Yet, because of the potential impact on hospital operations, unplanned IT downtime events can be just as serious a threat to patient safety as a power outage or medical gas failure. Therefore, it is essential that hospitals close this gap in emergency preparedness.

This toolkit is designed to assist hospitals and other healthcare organizations with improving their readiness for unplanned IT downtime events and is organized with the sections listed here:

- Recognizing the Scope of the Issue
- Collaborative Planning
- Multidisciplinary Response Teams
- Improving Response Tools
- Ensuring Efficient Communication
- Speeding Recovery
- Training and Exercise

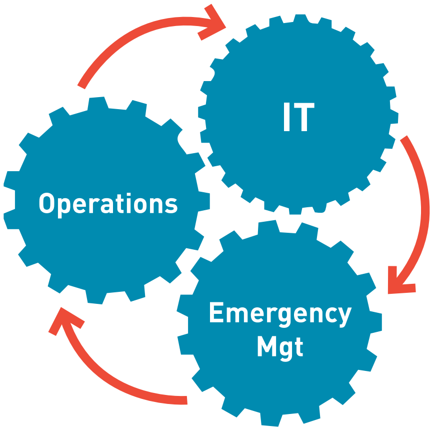
[1] Charles, D., Gabriel, M., Searcy T. (April 2015) Adoption of Electronic Health Record Systems among U.S. Non-Federal Acute Care Hospitals: 2008-2014. ONC Data Brief, no.23. Office of the National Coordinator for Health Information Technology: Washington DC.

/// Introduction

Hospitals and other healthcare organizations in the U.S. are adopting and utilizing information technology systems at an unprecedented pace. A recent survey of non-Federal acute care hospitals found that approximately 97% of hospitals now possess certified EHR technology, marking a 35% increase just since 2011.[2] This increasing adoption of IT in healthcare has been referred to as a "proverbial double-edged sword" (Palmieri et al, 2011), noting that IT introduces solutions to improve performance while simultaneously generating new potential problems, or "technical iatrogenesis" in already complex healthcare systems, especially when the new technology fails.[3]

In addition, IT failure events in healthcare can be extremely complex, with far-reaching, and sometimes unanticipated, disruptive consequences within an organization. As technology becomes an ever-more essential component of the delivery of modern medical care, healthcare entities must ensure that they have extremely robust and well-conceived operational plans in place to be able to identify the full extent and consequences of any outage as rapidly as possible. Healthcare providers must be prepared to support maximally safe and efficient clinical processes when their IT systems become unavailable.

For the purposes of this toolkit, we define an unplanned IT downtime event as any unexpected event where a technology system is unavailable, or fails to perform as designed. While many such IT downtime events are minor, either being invisible to end users and/or being fixed within minutes, some events have a much greater impact on clinical care and hospital operations, and these events can significantly threaten both the efficiency of clinical operations and the safety of the care delivered. Unfortunately, and importantly, it must be noted that the difference between major and minor downtime events is not always immediately clear, and it can require substantial effort to investigate both the full scope and the root cause of some unplanned downtime events in real-time.



The critical factor to successfully preparing for and managing IS downtime events in a healthcare environment is a having a strong system that supports and encourages collaboration among three key groups: IT experts, hospital operational leaders (such as nursing supervisors, administrators and others), and hospital emergency managers. These separate, but interconnected, groups must plan together, respond together, and recover together.

Assumptions and principles that underlie all of the sections ▶

[2] Charles, D., Gabriel, M., Searcy T. Adoption of Electronic Health Record Systems among U.S. Non-Federal Acute Care Hospitals: 2008-2014. ONC Data Brief, no.23. Office of the National Coordinator for Health Information Technology. April 2015. Washington DC.

[3] Palmieri PA, Peterson LT, Ford EW. Technological iatrogenesis: New risks force heightened management awareness. J Health Risk Manag. 2009;27:19–24. [PubMed]

While each section of the toolkit focuses on a different aspect of planning, response and/or recovery, there are certain assumptions and principles that underlie all of the sections:

- Despite the best efforts of IT leaders within a healthcare organization, it is inevitable that some IT systems will experience unplanned downtime events
- The full scope and clinical impact of downtime events may not be readily apparent when the event initially occurs
- Most hospitals tend to respond to IT disruptions in silos. An effective response depends on maintaining effective collaboration among all staff throughout the incident
- Maintaining situational awareness is notoriously challenging during downtime events, both for leaders and for end-users
- Major downtime events are true emergencies, and should be managed as any other emergency within the facility would be, by using the hospital's emergency plans and staff in response
- All staff must be able to autonomously transition into a downtime environment in order to respond to immediate patient care needs if their IT systems malfunction
- A successful transition to downtime operations requires that staff have well designed downtime tools readily at hand that mirror normal processes and systems to the greatest extent possible
- Downtime operations will never be as efficient or as safe as normal operations; hospitals must anticipate the key challenges that arise during downtime events and deploy mitigation measures and strategies to limit these challenges

/// Recognizing the Scope of the Issue

It can often be difficult for some hospital leaders, as well as for many end-users to fully appreciate the potential challenges they may face during unplanned IT downtime events. Sometimes this is the case because they take such systems for granted, but more commonly, it is because they typically have not entirely anticipated the consequences of loss of their systems. In addition, since IT utilization within healthcare continues to expand at an unprecedented pace, many have yet to experience a major and prolonged downtime event since they last added or upgraded key new systems or features, and therefore fail to realize how much more dependent on technology they are than the last time they had a system failure.

Risk Assessment and Mapping

In order to fully appreciate the potential scope of consequences that any unplanned downtime event can cause, it is essential to have a detailed map of both the technical and operational processes associated with each system, and to continually revisit and update those maps as new systems and features are added, and as operational processes change. Producing such maps in detail will likely require two parallel, but connected, programs.

The first program focuses on the technical side of planning, and involves recording how each piece of IT is dependent on other systems, servers, interfaces, switches, etc. within the network. This type of mapping and planning is most commonly addressed by an institution's Disaster Recovery (DR) experts. Disaster Recovery is a specialized discipline, often housed within an IT or business continuity department, that focuses on developing appropriate policies and procedures to enable recovery of technology infrastructure following any type of disaster event. DR experts are accustomed to producing maps of technical interdependencies within systems, and protocols for technological response to the failures of those systems. Although nearly all IT systems have some degree of DR maps and plans, not all of them are sufficiently detailed or current to be maximally useful 24/7/365 in the event of unanticipated systems failure. True collaboration requires shared tools that are understood by all involved.

The second program involves mapping the operational consequences of losing each piece of IT within the organization. While hospital leaders are obviously aware of whether their Electronic Health Record (EHR) systems support their institution's patient care records, patient tracking, and other functions related to direct patient care, many are not aware of the degree to which their other IT systems are also essential for other hospital services, such as materials management, utility services, security services, payroll, and communications. Without recognizing the full implications of losing each of the myriad of systems within the hospital's IT network, it is impossible to plan for appropriate mitigation and contingency efforts should any one or more of those systems fail.

It is only with such maps of both technical and operational interdependencies of IT systems in hand that hospital leaders and emergency managers can accurately complete their hospital's annual Hazard Vulnerability Analysis (HVA) for their IT systems. As all emergency managers know, completing an HVA involves systematically assessing the probabilities of the hazards that the hospital might face, the potential consequences of such hazards, and the institution's estimated existing preparedness for each hazard. In an HVA, the probability, consequence, and existing preparedness all factor into a composite score that describes and ranks the hospital's vulnerability to all of the hazards that they can imagine facing. For IT downtime events, while technical experts may be able to estimate the probability of system failures without additional assistance, it is impossible for them to adequately describe the operational consequences of those failures within the institution, or to describe the institution's readiness to respond to such failures without substantial input from other leaders and representatives from around the hospital.

Recognizing Vulnerable Processes

Certain routine operational processes within hospitals tend to become exceptionally dependent on IT services and systems that support them. In many systems, this can happen to a degree to which it is nearly impossible to complete these processes adequately without the supporting IT service. It is therefore important to be able to identify such processes in the assessment phase, so alternative plans and strategies can be developed. Examples of these processes include:

- Hospital inpatient admission
- Medication reconciliation systems accurately confirming patients' medication dosages
- Highly detailed order entry templates to ensure adherence to best practices
- Instances of patient movement and transfer within the hospital (which may rely on IT systems that prohibit clinical care if the patient is not "electronically" located in the correct unit/area)
- Hospital discharge (where systems support visit documentation, follow-up care and referrals, prescriptions, checklists of safety measures and communications with other caregivers)

Every hospital has unique workflows; it is important to have clearly developed alternative procedures in place that can support effective delivery of care when the IT systems that support specific vulnerable processes fail.

Prospectively Identifying Specific Threats to Patient Safety During Downtimes

From direct experience, or by learning from the experience of others, many clinicians have realized that there are aspects of clinical care that present a high risk of error when IT systems fail. Medication order entry systems that support dosage scrutiny, check for drug-drug interactions, and allergy alerting systems are obvious examples of systems designed to enhance patient care safety and whose loss is of special concern. However, there are also many other specific threats to patient safety during IT downtimes that may not be as immediately obvious, but nonetheless that must be considered in the risk assessment process. Among these threats may be: safely administering chemotherapy, selecting proper weight-based dosing for pediatric patients, ensuring adequate real-time access to prior medical records and results, and rapid communication of laboratory and radiology results to multiple clinicians.

Furthermore, since one of the principal reasons driving expansion of IT services in many areas of the hospital is the ability of IT to enhance patient safety, it can therefore be assumed that the magnitude of risks to patient safety may well increase in the future, as more technological safety systems are developed and have inadequate legacy downtime analogue practices. One potential strategy to mitigate this effect is to require that all new IT-based patient safety tools are reported to a downtime planning committee as they are developed, so they may have corresponding downtime procedures developed and tested. Incorporating Patient Safety representatives in the planning and response is critical to ensure through analysis of the patient safety risks.

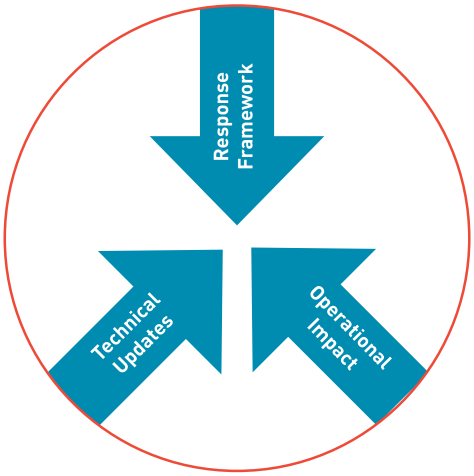
During a downtime event, leadership should implement measures to assess and assure patient safety in an environment with unavailable or unreliable systems. This may include implementing patient tracers and enhanced processes to report patient safety issues.

Anticipating the Magnitude of Operational Throughput Disruptions

The last feature of risk assessment for IT downtime events is to identify and potentially quantify the degree of operational disruption that an IT downtime creates throughout the institution. When IT systems fail, nearly every area of the institution that has been affected by the downtime becomes less efficient. This can be because of loss of the efficiencies that the system was designed to create, because of cumbersome work-around processes, because of a lack of staff familiarity with downtime procedures, or a combination of these and other factors. No matter what the reasons, however, most of the hospital will begin to experience delays and backlogs for the duration of the downtime. Some areas of the hospital with the greatest patient volume and/or patient acuity may be most affected by these operational disruptions and inefficiencies, such as the Emergency Department, operating rooms, intensive care units, and others. Laboratory and pharmacy services may also be severely affected. An optimal response to major IT disruptions may involve calling in additional staff to maintain throughput and quality and/or potentially limiting clinical services if throughput cannot be sustained. A hospital will benefit greatly if it can accurately estimate the degree of operational degradation any IT downtime can produce, so it can respond with enhanced staffing and other operational solutions appropriately in a time-sensitive manner. Leveraging an established Hospital Incident Command System (HICS) will expedite this process.

/// Enhancing Collaborative Planning

As mentioned above, it has been recognized that planning for IT downtime events is often siloed and/or insufficiently broad in many hospitals. Therefore, after a thorough risk assessment process, it is essential that hospitals develop and sustain a multidisciplinary downtime planning committee with broad expertise to be able to develop detailed plans and resources that meet the complex needs of departments throughout the facility should their IT systems fail.



The Downtime Planning Committee

Developing a downtime planning committee (or modifying an existing one) with adequate representation can be a daunting task, and the logistics of determining the optimum size of the committee and identifying appropriate individuals to participate will take time. While adequate expertise generally exists at every hospital, the challenge is finding the right range of individuals who have an understanding of the intersection of the technical and operational processes in their department and/or field of expertise to adequately represent the whole institution.

In general, an ideal multidisciplinary downtime committee will have representatives across these categories of disciplines: IT experts, emergency managers, and operational leaders.

- Operational managers and leaders must always be included to represent the "front lines" of the institution. They provide a conduit to the committee for end-users' concerns about downtime planning and response, and also from the committee to end-users to ensure new initiatives are understood and accepted by all. While they do not necessarily need to be IT experts themselves, selected operational representatives should have a basic understanding of the IT systems and services that support their departmental operations, and a rudimentary technical vocabulary. In addition, there should be sufficient operational representation on the committee to reflect the breadth of institutional services, in both direct clinical and supporting departments.

- IT experts obviously must be included to incorporate their knowledge of the technical details of system operations into planning efforts. It should be noted, however, that not all IT staff will have equal expertise or familiarity with all of the hardware and software supporting the range of institutional systems. Therefore, several IT experts may be required on the committee. In addition, since many hospitals use outside vendors and/or contracted systems as part of their IT services, it may be advisable to include key outside vendor representatives in planning committees when their expertise is of value, and especially if those vendors will be required to participate in a downtime response.

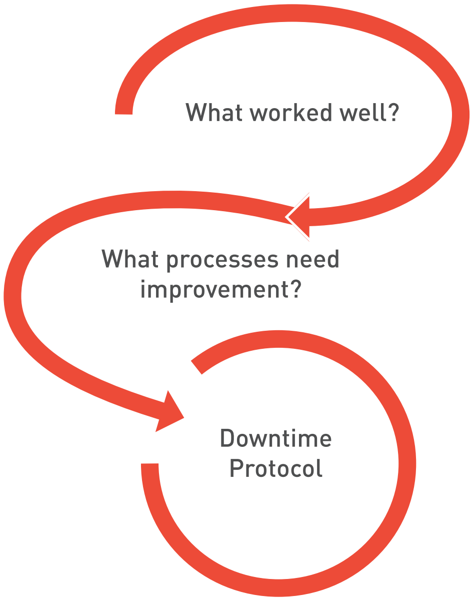
- Emergency managers can ensure that downtime plans and protocols are consistent with the overall institutional Emergency Operations Plan (EOP). They can also help ensure that the committee addresses all of the typical phases of emergency management: mitigation, planning, response and recovery.

Some of the suggested representatives on a Downtime Planning Committee include those from the following services and departments:

- Information Technology
- Informatics
- Emergency Management
- Admitting Office
- Staff Physicians
- Nursing
- Labor and Delivery
- Pathology and Laboratories
- Pharmacy
- Emergency Department
- Nutrition and Food Services
- Patient Safety
- Outpatient Clinics
- Operating Rooms and Procedural Areas

The downtime planning committee should be asked to review the institution's IT risk assessment on an annual basis, in order to inform their discussions on the year's priorities for action. As mentioned before, the committee should also perform detailed reviews of the potential consequences of failure of any new system or technical safety initiative that is added to their hospital's IT portfolio over time.

The committee's routine work should focus on producing strategies and tools to more effectively mitigate and respond to unplanned downtime events. The committee should continually strive to identify ways of making downtime events invisible to the patients, and ideally to the front-line system users as well. Doing this involves continually developing better downtime tools for users (see the next section of this toolkit), and also realistically recognizing where additional non-technical resources are needed for a safe downtime response. For example, a downtime committee may develop a better paper-based process to be used when ordering medications from the central pharmacy during downtimes, but the committee may also point out to leadership that a specific number of additional pharmacists and technicians will be required during a downtime to ensure safe medication administration.



In addition to its routine planning activities, the downtime committee should perform a critical review of all unplanned downtime events in order to identify strengths of each response, as well as items for improvement and areas in need of further planning. Downtime committees should perform root cause analyses of downtime events, and focus on identifying and describing all of the safety, throughput, and other patient care consequences that have been caused by each downtime event. As always, staff are encouraged to capture patient safety concerns via the hospital's reporting systems, and should have specific training on how to bring identified issues of concern from those systems to the broader committee to be addressed.

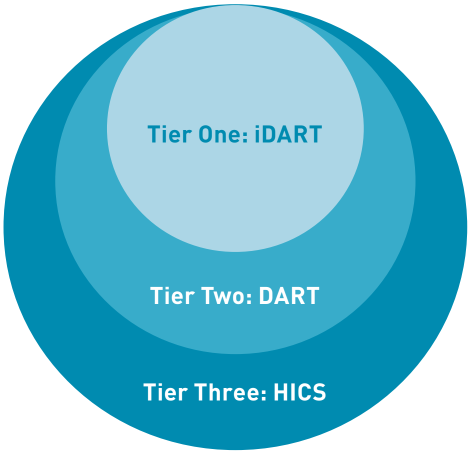
All of the hospital's downtime protocols and tools should be continually re-assessed and improved as necessary based upon lessons learned from exercises and real downtime events.

/// Developing Multidisciplinary Response Teams

A previously discussed, while many hospitals may have a downtime planning group or committee (not uncommonly with rather limited non-technical representation), very few have dedicated multidisciplinary teams with IT, clinical, and emergency management experts that are specifically designed to respond to downtime events in real time when they occur.

Unfortunately, trying to use a downtime planning committee to respond to a sudden downtime event as it occurs may not always be successful. First, since planning committee members are commonly comprised of day-shift staff, it may be difficult to assemble sufficient representation from the committee rapidly to respond effectively to an off-hours event. Indeed, many members of the committee may not have formal on-call responsibilities, and therefore may not be (or may not wish to be) reachable at all hours. Second, committee structures can be cumbersome to convene and manage when investigating the scope and scale of ill-defined events in the midst of a crisis. Pre-defined call lists may not exist to quickly activate and convene the committee members, and committees may lack the mechanisms to support rapidly sharing situational updates and other information. Lastly, because large events may actually necessitate formal activation of a hospital's emergency operations plan (EOP) and use of the Hospital Incident Command System for incident coordination, it can be unclear how a downtime planning committee is best integrated ad hoc within these plans and systems.

Therefore, to avoid the problems above, and to support a more effective response to unplanned downtime events, we suggest the creation of a tiered downtime response system that allows for sufficient flexibility to adjust the response based on the unique needs of the event.



Tier One: A small, multidisciplinary team is initially notified of unplanned downtime events in real time, to assess the operational impact of the event. The team then decides what type of response (if any), is warranted.

Tier Two: If the initial response team determines that the downtime incident does indeed affect hospital operations, a dedicated multidisciplinary response team is activated to manage the incident.

Tier Three: If the initial response team determines that the downtime incident is having a major impact on hospital operations, the hospital activates its emergency operations plan. Events may also evolve from a Tier Two to a Tier Three level of activation if the scope of the downtime expands and/or the understanding of new operational impacts grows. On some occasions a significant downtime event may warrant an immediate activation of the Emergency Operations Plan, there is no requirement that the response move through the tiers sequentially.

The Tier One Response Team (iDART)

This small team of specially selected representatives, sometimes called an initial Downtime Assessment and Response Team (iDART), helps to facilitate a rapid assessment of each unplanned downtime event. The group's primary objective is to assess if there is (or is likely to be) a noticeable impact on any part of hospital operations during the incident.

One of the greatest challenges in developing a Tier One, or iDART, plan is determining which events require activation of the team. As all IT leaders know, brief malfunctions or errors within IT systems are extremely common, and many self-resolve and/or are fixed quickly without ever being noticed by end-users. Indeed, it would be inappropriate, and would likely quickly cause activation fatigue, if the IT leadership were to notify an iDART with every small failure of an IT application, server, or other system. Therefore, it is important to attempt to create iDART activation criteria that are carefully worded. Some example iDART activation criteria are listed below, but they may need to be tailored for each hospital environment.

- Any IT failure of one of the critical clinical applications of the hospital (registration, documentation, order entry, results reporting, patient tracking, etc.)
- Any IT failure that disrupts communications within the hospital (i.e. email, paging, telephony (via Voice Over IP), etc.)
- Any IT failure that may affect business continuity before it is expected to be resolved (i.e. payroll, accounts payable, human resources systems, etc.)
- Any IT failure that causes a patient safety or other concern to on-site leadership (i.e. nursing supervisor)
- Any IT failure that causes concern to IT leadership (i.e. IT Administrator on Call (IT AOC))

For membership, the Tier One, or iDART, team must collectively have a diverse knowledge base, spanning knowledge of both the technical systems of the hospital as well as overall hospital operations since their goal is to quickly identify both specific technical problems and their functional impacts. Keeping the group small enough, however, as to not become unwieldy or excessively disruptive to overall hospital operations is a counterbalancing challenge. A sample list of possible iDART members is below:

- IT Administrator on Call (IT AOC)
- Hospital Administrator on Call (AOC)
- Nursing supervisor
- Emergency department charge nurse (or other ED representative)
- Emergency preparedness manager on call
- Admitting office
- Informatics clinicians (RNs and/or MDs who specialize in the use of IT within the hospital)

Once notified of an incident, the individual iDART members should immediately query key users on the front lines of the hospital to assess the impact to normal operations. Shortly after activation, the iDART members will report the results of their queries and discuss the incident details.   A sample iDART activation message, timeline and call agenda are listed in Appendix I. If the iDART determines that the incident can be resolved quickly without any disruption to hospital activities, then the group will focus on communication and monitoring the situation until it is fully resolved. However, should the iDART determine that the incident requires specific actions of employees or managers outside of the IT department, the iDART should automatically escalate their response to a Tier Two or Tier Three level. Hospital emergency management staff on the iDART can help moderate group discussions and facilitate decision-making about the appropriate next steps, as they would for any other emergency event.

The Tier Two (DART) Team

Any unplanned IT disruption that is sufficient to require response actions outside of the IT department, but that is not large enough to need activation of the hospital's emergency operations plan (EOP) should be managed with a multidisciplinary team, sometimes called a Downtime Assessment and Response Team (DART). The purpose of creating a DART is to support both rapid hospital-wide assessment of the downtime impacts, and also rapid response.

The Tier Two team/DART membership is comprised of the members of the iDART and other key service line leaders within the hospital. A sample example of a full DART membership list is below:

- All iDART members
- Labor and delivery manager/representative
- Operating room manager/representative
- Pharmacy manager/representative
- Laboratory manager/representative
- Radiology/imaging manager/representative
- Outpatient practices manager/representative
- Nutrition and food services manager/representative
- Police and security manager/representative
- Buildings and grounds/facilities manager/representative
- Materials management manager/representative
- Research operations (if applicable) manager/representative

While it is desirable that the DART members above have a basic understanding of the IT services and systems used within their departments and service areas, it is not essential that they are technical experts. Instead, it is extremely important that they have redundant mechanisms to communicate quickly with their staff who are on the front lines, both to gather further details about the problems caused by the outages and also to share response actions that are developed by the DART as a whole.

Like the iDART, the DART is supported by hospital emergency management staff, who support assembling the group (typically virtually), moderating discussions, ensuring situational awareness, monitoring the effectiveness of response actions and documenting key actions. Once activated, the DART will convene to quickly assess the operational impact of a downtime event and focus on:

- Determining the scope of the issue and all anticipated and/or known impacts to hospital operations
- Identifying IT and hospital operational response priorities and objectives
- Assessing resource needs
- Implementing a communication plan for staff, patients, and other stakeholders
- Directing, monitoring and evaluating response actions
- Determining if the incident requires escalation to a full HICS activation

By formally transitioning the usual responsibilities during downtime response to a broader DART, IT leaders are more able to focus on the technical aspects of downtime response, and operational leaders are more attuned to any safety and throughput concerns that may arise as they occur. This approach therefore capitalizes on the complimentary skill sets of a diverse team.

The Tier Three (HICS) Response

As already mentioned, because of the ever-increasing reliance on IT within hospitals, it is quite possible that an unplanned IT downtime could cause such significant disruption to hospital operations and to patient safety that the event requires activation of the hospital's Emergency Operations Plan. In these situations, use of the hospital's pre-established incident management structures, such as Hospital Incident Command System (HICS), is recommended in order to provide a comprehensive framework that supports rapid, institution-wide response and effective communication by leveraging a systematic approach driven by clearly defined objectives and goals.

The principal sections of the Hospital Incident Command System ▶ are identified on the next page.

The principal sections of the Hospital Incident Command System are identified below.[4] HICS defines these sections so that the various roles and responsibilities of an effective emergency response are clearly identified, and to ensure a comprehensive response plan is developed and implemented.

HICS Position	Role Description	Key Objectives
Command	• Sets the incident objectives, strategies, and priorities and has overall responsibility of the team/incident • Responsible for all functions, may elect to perform all functions or delegate them out • Delegation does not relieve the Commander from responsibility	• Lead overall response • Establish response priorities/objectives • Lead Briefings • Advocate for rapid resolution of technical issues • Ensure diligent monitoring of patient safety, address potential concerns immediately
Operations	• Conducts operations to carry out the plan • Develop the tactical objectives and organization, and direct all tactical resources	• Continue safe patient care • Round in all clinical areas to monitor for staff fatigue • Identify additional resource needs and coordinate with the Logistics Section Chief to secure and distribute resources (ex: prescription pads to hand write patient prescriptions upon discharge)
Planning	• Collect and evaluate information, maintain situational awareness and documentation for incident records	• Draft and distribute Incident Action Plan documentation • Monitor census / capacity in light of inefficiencies related to the downtime event • Organize labor pool to assist with manual processes (ex: delivering printed lab reports)
Logistics	• Provide support and all other services needed to meet the operational objectives • Equipment, supplies, transportation, food, water, and shelter	• Provide information, including technical updates related to downtime resolution • Ensure adequate supplies to support staff respite (cots, food, water)
Finance	• Monitor costs related to the incident	• Track costs related to additional staff needs and overtime hours • Calculate service recovery costs

[4] Hospital Incident Command System Guidebook, 2014. The California Emergency Medical Services Authority (EMSA). http://www.emsa.ca.gov/media/default/HICS/HICS_Guidebook_2014. Accessed February 2017.

With respect to the effective use of HICS during major downtime events, it is important to remember the following:

- Even when using HICS, many hospitals can experience "siloing," with clinical/operational information and actions managed within the HICS structure, but IT information and decision-making being managed within a parallel system. It is essential to define a clear path within the HICS framework to support two way communication for IT leadership to communicate technical details and updates about the downtime to the specific leaders throughout the hospital and for information to flow back from end users, up through HICS to IT leaders and managers.
- In an IT downtime event, the principal goals for the Operations Section Chief are 1) to identify and address safety threats caused by the downtime and 2) to monitor operations for throughput challenges. Achieving these goals may be especially challenging when the usual systems that supply data about operations are computerized and may not be functioning. The operations section must have pre-developed protocols for monitoring hospital occupancy, throughput, and safety challenges that can be deployed in a downtime. Moreover, in order to respond effectively, the Operations Section Chief should have a rough idea of the magnitude of additional human resources that may be required to be called in when IT systems fail in each critical area of the hospital.
- The Planning Section within HICS is charged with monitoring the situation status during a response and distributing situational updates. There must be mechanisms in place that support excellent information sharing from IT leaders with the Planning Section and include the "translation" of information into a non-technical summary. In addition, because communications systems such as email and others may be affected by the IT outages, Planning Section leaders must have pre-planned mechanisms to communicate outside of email systems, or other traditional means. All messages must be appropriately vetted by technical experts and the Incident Commander.
- Other members of the iDART and DART will likely be required to participate in the incident response in a full hospital EOP activation. Each team member should clearly understand his or her role in the hospital's HICS structure and how she or he should report and respond to the IT downtime event.
- The institution should consider the possibility of cyberterrorism or other malicious acts in its planning for the use of HICS in a downtime event. While some of the effects for the end-users may be similar with respect to systems that are compromised, the information security, physical security, reputational, and other questions that may be raised in a cyberterrorism event are substantially more complex.

Planning for cyberattacks should also include the following considerations:

- Vulnerable systems: Complete a comprehensive review of all devices that connect to the network, including personal laptops, unsecured medical devices, diagnostic devices a vendor may bring onsite, ATM's on the property
- Compromised systems: Whether it is possible to isolate an affected system and allow other work to continue elsewhere on the network
- Notifications: In addition to internal event notifications, planning should incorporate notification to law enforcement (local, state, and (FBI Cyber Task Force). Law enforcement can advise when to report to regulatory agencies as this may interfere with criminal investigations. US HHS provides the following guidance: https://www.hhs.gov/sites/default/files/cyber-attack-checklist-06-2017.pdf

/// Improving Response Tools

Developing Appropriate Resources

An overarching hospital downtime response protocol, based on real lessons learned from internal and external responses is absolutely required to guide an effective hospital response to downtime events. In particular, the protocol should strive to define, how differing IT incidents are classified (i.e. major vs. minor events), how notification of events is escalated throughout the system, how known anticipatable safety and operational challenges can be mitigated and addressed, and what essential actions must be taken or considered at each phase of the response.

It is at least equally important, however, that front-line staff possess effective tools and other resources to continue their actions safely and effectively during a downtime, and that they have the instructions necessary to properly use them. No front-line clinician will have the time to read through a detailed "downtime plan" when their systems fail them, and therefore they all require readily accessible checklists, forms and simple tools that can help to ensure as smooth a transition in care as possible from "up" to "down."

In many hospitals, it is not uncommon for their "downtime forms" to consist of boxes of legacy paper forms and requisitions that are holdovers from a time well before electronic systems existed. As a result, the "downtime" paper forms may look nothing like the current electronic screens, menus, and forms with which the end-users are much more familiar and comfortable. This creates a "double-whammy" during downtimes where front line nurses, physicians, and others are then not only deprived of their efficient technology, but also must decipher and use backup tools that are substantially different from their typical work environment.   Hospitals may be much better served when their downtime documentation, order entry, and other forms are regularly reviewed and updated to mirror their current electronic systems' format.

While clinical care begins at the bedside, it often continues into a pathology lab, a pharmacy, radiology suites, and other critical areas. Downtime tools must be developed that support the operations of all of these services. Moreover, other aspects of a hospital's operations that are not strictly "clinical", such as food service or materials management, but that rely in electronic systems must all have similarly intuitive downtime forms and procedures. A comprehensive planning process must address the diverse needs of all hospital departments and disciplines, and take into consideration the impact on patient flow across the continuum of care.

Utilizing the following items on the following page may be helpful as a hospital refines its downtime response protocol, and tries to create improved tools and resources for response: ▶

Downtime Manual	Include checklists and quick reference instructions that are available in a central, visible location for staff to utilize during downtime (consider using a red binder). Specifically address the key areas of vulnerability for the unit, including patient tracking, documentation, order entry, results reporting, and communications with others in the institution. Ensure that every unit has simple instructions within the manual that support their transition to downtime operations and offer clearly identified criteria and mechanisms for escalating downtime problems and concerns. Because results reporting can be especially problematic during downtime events, especially in busy units, ensure that the manuals clearly describe reporting laboratory, radiology, OR procedure specific case cards and other department specific tools identified by end-users. Include other tools to assist with clinical unit operations such as key phone numbers.
Failsafe / Business Continuity Access Computers	Business Continuity Access (BCA) is comprised of designated failsafe computers that connect to the network and receive patient chart information on a set interval (ex: every 15 minutes) and save the data to a file on the hard drive. These devices serve as a way to review historical data on each patient, but cannot receive new data or updates until the system is restored. Consider policies or systems for automatic printing of essential information from the failsafe computer when there are concerns that the failsafe computers may lose power or may also malfunction.
Paper Forms	Forms that support ongoing clinical care and other unit operations while the IT systems are not functioning. All forms should closely mirror on-screen resources. Consider keeping the templates for these forms as a saved file on the Failsafe Computer, but ensure a sufficient supply is printed in the Downtime Manual.
Online Communication Portals	Assuming the Internet remains functional while other systems are down, availability of an online portal to interact with staff allows leadership to communicate real time information and updates to downtime resources.
Medical Reference Texts	As more and more medical information (becomes electronic, paper-based textbooks may be essential to assist clinicians with drug dosages, interactions, and other protocols.
Reconciliation and Recovery Instructions	Instructions on how to recover from a downtime event, including how to address documentation and other challenges that may have occurred during the event. (See the section on next page for greater specific discussion of Recovery from downtime events).
Other Tools	Ensure that sufficient paper-based tools are available to support the full spectrum of clinical resources that are normally electronic on a unit, such as admitting order sets, discharge procedures, outpatient referral systems, outpatient prescription pads, discharge care information, and others.

One best practice observed at a Boston-area hospital is the development of "Downtime Code Carts" located on each unit.[5] These one-stop-shops for all of the downtime resources required by the staff on a unit are not only exceptionally helpful in speeding the transition to safer downtime care, but they are also symbolically important, reflecting the potential true safety crisis that can emerge during a downtime event. Like other code carts, they can be equipped with break-away locks to clearly indicate when they have been used, and are in need of resupply. If hospitals do not adapt the "downtime code cart" idea, they can similarly wrap their response binders in removable clear plastic for the same purpose.

Planning efforts must take into account that staff efficiency will be impacted by a downtime event; the longer the duration, the more significant the impact. Downtime processes will impact all aspects of patient care; patient registration and intake will take longer to process on paper, physicians will take longer to enter orders, and labs, radiology, and pharmacy departments will take longer to process orders and share results. Many staff members will not be accustomed to using these paper forms. The use of "runners" to deliver forms, waiting on busy phone lines for results, and manually looking up supply locations in stock rooms, will all impact the efficiency of patient care and result in a longer length of stay.

[5] Nigrin, Daniel J. MD, MS, Senior Vice President Information Services Department and Chief Information Officer, Boston Children's Hospital. "Harvard Clinical Informatics Lecture Series." 26 Sept. 2016, Boston, Massachusetts.

/// Ensuring Efficient Communication

Communication during any emergency event is critical to ensure accurate situational awareness, to provide coordinated instruction to those affected by the incident, and to combat the promulgation of falsehoods. However, as mentioned previously, it is notoriously difficult to preserve effective communications and to maintain sufficient situational awareness within a hospital during IT downtime events, even if the principal communications systems, such as email, are not compromised. If the hospital's communications systems are also affected, it is even more difficult to do so. A strong, multifaceted, and flexible communications strategy is an essential element of downtime planning, and will enhance all aspects of a response protocol.

Redundant and Effective Communication Systems

Hospitals should map their diverse network of communication systems and the vulnerabilities of each system in order to ensure that communication channels are available at all times. A downtime protocol should consider how various forms of communication may be affected during different types of downtime events (such as loss of internet, loss of power, loss of data centers or servers, telephony or others) and what kinds of information sharing are likely to be affected. Similarly, hospitals must consider how their clinicians are likely to receive information during an actual event. For example, many clinicians may not access their email during a downtime event, especially in the Emergency Department or in the Operating Rooms, and alternate methods of communication must be used. Some hospitals have begun adopting technology that allows them to broadcast a message onto all of the computer screens in the institution as long as their intranet is functioning. Hospitals may wish to focus special attention on the systems needed for incident leadership, mass messaging, results reporting, and patient tracking. All hospitals should have "analog" (i.e. paper-based, human-based or other non-electronic) means of supporting communications in these areas as their ultimate fall back plans in case of massive system failures.

Sending Accurate and Timely Messages

Pre-scripted communication templates can help leverage communication tools more effectively during a response, especially with the initial notification of a downtime event to a large end-user audience. However, it is not always clear which incident responders should send out a "downtime" message, or when. For example, it may be fastest for an IT professional seated at the Help Desk to send out an all-user email that the central pharmacy's system is down, but he or she may not be able to tell users what to do in response to that outage. Conversely, a hospital's leadership may recognize that the pharmacy system is down, convene their management teams, carefully script a message to all users, only to have the event resolve by the time they have finished all of their meetings and made all of their decisions.

Timely messaging will help empower front line staff to use the resources available in the department to continue to provide safe and effective patient care. Collaborative messaging will ensure that the information communicated is technically correct, and operationally relevant. The challenge lies in trying to be both timely and accurate when many events are initially unclear in scope, cause and anticipated duration.

An organizational philosophy that supports early activation of appropriate leadership teams for IS downtime events, even when such activation is occasionally not necessary in retrospect, will best support early messaging when it is needed. With early messaging, staff actions are more likely to be coordinated as the event progresses, and safety risks are minimized. Without clear messaging, staff may choose to act on their own, and be tempted to begin to modify or delay care and clinical interventions to "wait out" a downtime which may have serious consequences during an event.

Responding to Extended Events

At the onset of most downtime events, the time that will be required for resolution of the incident is often unclear, however most downtime events are resolved relatively rapidly, within minutes to a few hours. However, as certain events linger past a few hours, the stresses of sustaining an emergency response in the hospital and for staff using manual processes will build, negatively affecting staff and patients. Planning for staff support should include a process to monitor for staff fatigue as in any major emergency response, long hours, extended events, the burden of manual processes, patient frustration may all contribute to staff fatigue. Staff support must account for roper rest, time off the unit, food and water. Plans for strong two-way communication will also help to ensure that questions are answered, resources are available to help manage patient care, rumors are minimized, and staff feel supported.

/// Speeding Recovery

It has been suggested that organizations should strive to consider their recovery needs at the start of any emergency incident to help ensure the organization is able to return to normal operations as quickly as possible. This is especially true for IT downtimes due to the nature of clinical data reconciliation. For example, when an order entry system is re-activated, there may be pending orders visible on the system from the start of the downtime, and the clinician may not recognize that the medication has already been documented as administered on the paper forms now in the patient's chart. Without careful recovery and reconciliation processes, there would be a risk of excess medication administration in this example. Therefore, in contrast to many other kinds of disasters, the period of recovery can be one of special patient safety threats following an IT downtime, and requires special planning and management to navigate well.

Patient Safety Considerations during Reconciliation

Data reconciliation entails manually transferring detailed patient data into the online system. During this data reconciliation process, each step must be planned and monitored for accuracy to ensure patient safety. Some key issues to consider in this process include:

- The process of medication order entry reconciliation after downtime is especially prone to errors and must follow a strict protocol during recovery.

- Downtime forms must be carefully reviewed to ensure the data captured on paper is correctly aligned with the sequence and format of the data entry process in electronic clinical systems.

- Paper charts documenting clinical interventions, care, and progress must be available to multiple clinicians simultaneously as quickly as possible after the downtime so that care can continue effectively. In some cases, document scanning capabilities may limit the reconciliation burden, but in all cases the verifying of data integrity is labor intensive and time consuming.

A well-coordinated recovery plan will minimize the safety risks associated with reconciling patient records. Recovery efforts must account for exact reconciliation needs ahead of time to properly allocate resources necessary for data entry and quality assurance oversight. Reconciliation is often a coordinated effort, data must be entered in a particular sequence while IS personnel monitor the server capacity and data moving between systems as they come back online.

Coordinating the Recovery Process

Regardless of the size of the event, all members of the response team must understand that patient safety concerns persist throughout the recovery process. A consistent approach to recovery will minimize the risk, therefore the response protocol must include detailed instructions to guide the reconciliation effort. The response team will play an important role in the coordination of various departments as they enter information to different parts of a patient record.

Service Recovery

Despite best efforts to support a seamless transition to downtime protocols for patient care, some patients may experience longer wait times for results, delays or cancellation of appointments. Acknowledging this impact will assure patients that the changes they observe will not have any lasting impact on the care they expect to receive from the institution. Service recovery is equally important for staff. The lowered productivity and slower throughput caused by a downtime will cause frustrations as staff try to complete daily tasks. It is critical that leadership consider staff morale throughout an extended event. Leadership should consider including speaking points to answer questions that originate from staff, patients, and visitors to explain downtime procedures in a simple, straightforward manner.

/// Training and Exercises

A well-developed training curriculum will consider the unique needs of varied staff populations. A subset of staff may be accustomed to leveraging downtime tools during regular planned downtimes related to system maintenance; off-hours staff may have fewer resources to assist with reconciliation and recovery; and weekend shifts may not have the benefit of leadership presence. While planned downtime events offer a cost effective opportunity to practice downtime protocols, they will likely occur on a regular schedule, thus only reaching a narrow representation of staff. If most planned maintenance outages are scheduled for Sunday overnights, then only staff that work on Sunday overnights will be exposed to the process on a regular basis. It is imperative that all staff, on all shifts, are able to recognize a significant systems issue, and take immediate steps to activate a downtime response protocol.

A robust training program for IT downtime events incorporates a variety of modalities to provide staff with the knowledge they need to respond effectively. Such programs use classroom training, followed by workshops and tabletop exercises to simulate an IS downtime event and allow a safe environment to practice response actions. More advanced forums including full scale and functional exercises expand the scope and detail of exercise play as described below.

Exercises

While planned downtime events offer a unique opportunity to test a portion of downtime response protocols, they do not offer the full benefit of a well-designed exercise program. A well-executed exercise allows a thorough examination of all aspects of a downtime protocol and permits participation from a broader audience to assess the protocol and identify potential gaps in planning.

Planning, training, and exercises should mirror the tiered response expected during an unplanned event. Consider the following approach:

Standard, predictable downtime events with a minimal organizational impact should provide opportunity for all relevant subject matter experts to practice their roles identifying the scope and impact of a downtime, identifying potential patient safety concerns, and activating relevant response protocols and associated communication plans. Planned downtime events provide an excellent training opportunity.

In general, there are four progressive levels of action in an exercise program:

- Drills test a single specified operation, such as activating a notification system or measuring response times. In contrast, exercises test multiple operations.

- Tabletop exercises are low stress events designed to identify major gaps or conflicts in planning. Participants discuss which actions they would take when faced with a given downtime event, but no real resources are used.

- Functional exercises are higher fidelity events where many participants simulate their actions in a response environment and must make immediate, specific decisions, but real equipment and personnel are not deployed.

- Full-scale exercises are the most realistic, most complex, and costliest events where personnel perform as many of their actual duties as possible in a simulated emergency in order to best assess the true capabilities of the response system.

Hospitals' increasing reliance on integrated electronic health records means that staff are less familiar with hand written orders, flow sheets, and prescriptions documented on paper. Drills and exercises are an important tool to ensure all clinical staff have, and maintain, these important skills so they are able to function effectively during unplanned downtime events.

Evaluation

After each drill, exercise, or real-world event, it is critical that the hospital facilitate a debriefing session to capture best practices to carry forward, and identify areas of concern to evaluate further. Every opportunity to capture lessons learned will strengthen a protocol. For planned events, drills, and exercises it is important to identify clear objectives and measure the outcomes against those objectives. The standard best practice for documenting these results is an After Action Report, as this provides a consistent format for those involved to review the composite feedback and resulting updates to the plans and protocols.

Part of the evaluation process should include collection of feedback from staff throughout the organization who were involved in the event. Whenever possible, staff affected should be invited to debriefing sessions to share their experience and offer suggestions for improvement. Including staff in this manner empowers them to feel part of the improvement process, and increases their ability to respond effectively to future events.

/// Conclusion / Summary

This toolkit is designed to accommodate the unique aspects of each hospital and is intended to serve as a framework within which an individual program may grow. Despite different settings and capabilities, the expertise to respond to unplanned downtime events already exists is some fashion at many institutions. This toolkit is meant to facilitate productive collaboration and encourage a more thorough understanding of the interplay between the technical and operational aspects of patient care and hospital operations. The shared experiences of Information System departments, Emergency Preparedness staff, and operational stakeholders will guide the development of a planning committee and assessment team that are able to seamlessly integrate into the hospital's formal response structures.

Appendix I:

Summary of Downtime Planning and Response

- Clinical Downtime Committee: A diverse team of subject matter experts from both IT departments and clinical teams that collaborate to improve planning for scheduled downtime events

- Downtime Assessment and Response Team (DART): This team exists to support IT Leadership during unplanned downtime events by conducting a rapid assessment of the scope of an unplanned downtime event and developing a response to mitigate operational impacts

- The Initial Downtime Assessment Team(iDART) is a smaller subgroup of DART to help identify when there is an issue that requires assessment and response

- Incident Management Team (IMT): This is a multi-disciplinary, hospital-wide response structure; used to respond to all hazards (e.g., downtimes, blizzards, utilities failure, mass casualty events, etc.)

- Hospital Incident Command: It is possible a significant unplanned downtime event could impact patient safety to the extent that the event requires activation of the hospital's Emergency Operations Plan

Type of Downtime Event	Response Team	Key Points
Planned Event	Clinical Downtime Committee	• Larger standing committee • Diverse representation • Operational knowledge
Isolated Event	IT Leadership	24/7/365 coverage
Unknown Impact	IT Leadership AND Initial Downtime Assessment and Response Team (iDART)	Very small group to rapidly assess if there is an issue
Known Impact	IS Leadership AND Downtime Assessment and Response Team (DART) AND Incident Management Team (IMT)	• Trained response team • Diverse representation • Operational knowledge • Onsite representation • Hospital AOC
Significant Impact	Hospital Incident Command System	Full disaster response

Appendix II:

Developing a Downtime Planning Committee

Sample Mission Statement:

The Downtime Planning Committee is tasked with improving the planning process for scheduled IT Downtime Events by encouraging collaboration between IT experts, key operational leaders, and emergency preparedness staff; bringing together diverse perspectives to improve communication prior to known downtime events.

Potential Stakeholders:

- Information Systems
- Emergency Preparedness
- Clinical Informatics
- Emergency Department
- Direct Admit Services (ex: Labor and Delivery)
- Patient Care Services
- Pathology
- Pharmacy
- Radiology
- Nutrition and Food Services
- Outpatient Operations
- Patient Safety

Forming the Committee

- Represent diverse, key areas of the institution
- Have enough technical knowledge to understand how systems share information, and be able to assess peripheral impacts of a downtime event on the systems his/her department rely on as part of daily operations
- Be available for regular meetings (ex: monthly or quarterly) to discuss scheduled downtime events

Sample Committee Objectives

- Review planned downtime events (ex: scheduled server maintenance, updates, new software) to ensure the scope and time are set to minimize impact to clinical operations
- Develop and refine mitigation plans to address unavoidable impacts, including downtime procedures
- Discuss communications planning to alert staff before, during, and after scheduled events in a clear concise manner that highlights key aspects of complex technical work as it relates to operational impacts

Appendix III:

Developing a Downtime Assessment and Response Team

Sample Mission Statement:
The Downtime Assessment and Response Team (DART) is a mutually beneficial structure supporting IT Leadership in assessing the scope of the unplanned downtime and supporting the affected departments by ensuring their challenges and needs are made known to leadership. A DART does not replace established Downtime Committees, nor any other response group; the DART is an important resource to quickly assess the scope of a downtime event and identify potential impacts to patient care or other business operations. Ideally the DART is a subset of the Downtime Committee.

Forming the DART

- Representatives shall have enough technical knowledge to understand how systems share information, and be able to assess peripheral impacts of a downtime event on the systems his/her department rely on as part of daily operations
- Representatives must have availability to discuss their operational area 24/7/365. Therefore, DART representatives may include virtual/on-call pagers, primary and backup representatives, or similar arrangements to ensure coverage off-hours or through vacations, etc.
- The team should be small enough (e.g., no more than 10-15 individuals) to ensure the downtime assessment call is both efficient and effective

Sample Process for DART Response Activation

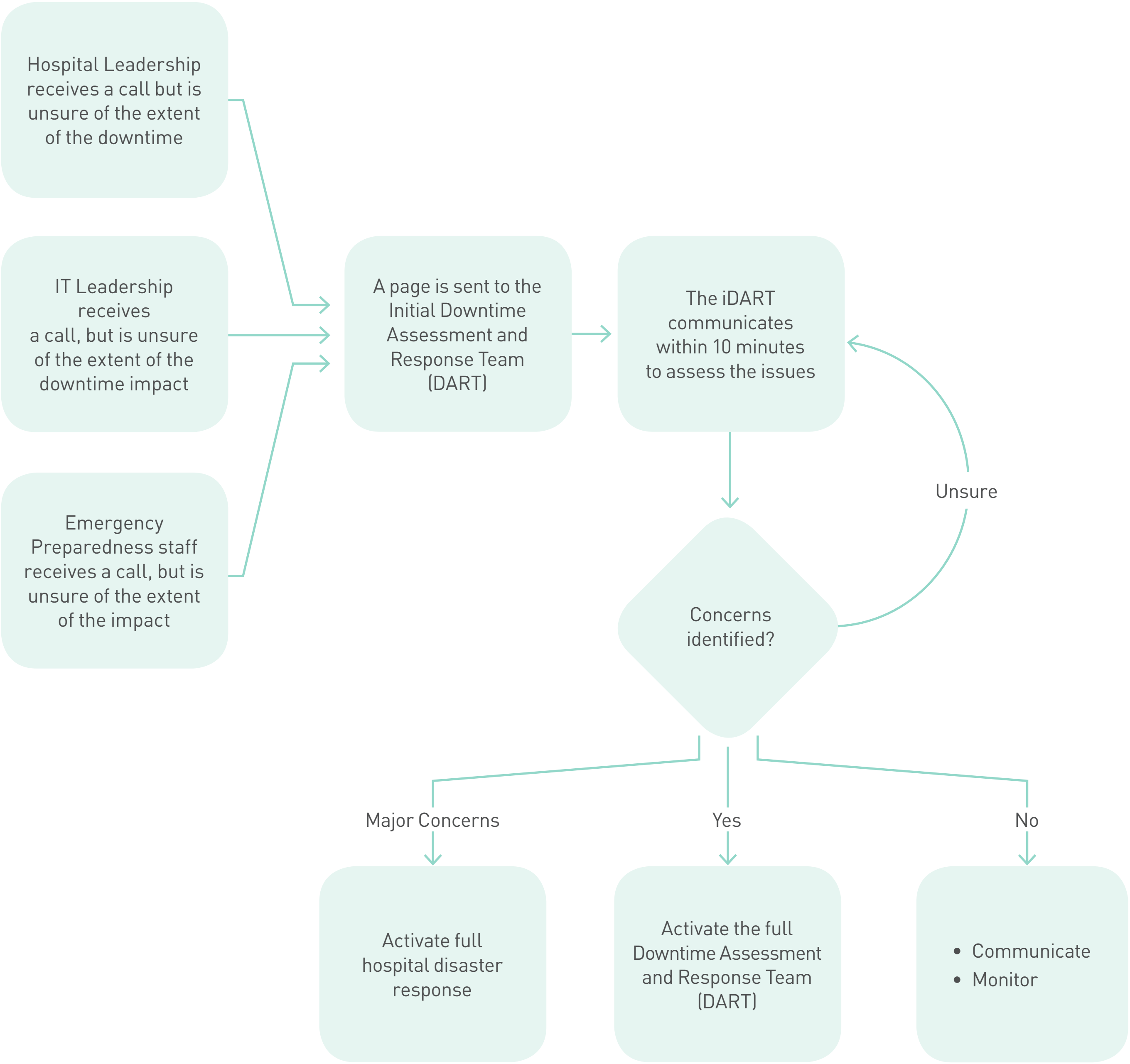
- The DART will activate when there is an unplanned downtime event requiring feedback regarding system status and interconnectivity
- The DART will meet virtually (i.e., conference call) within 10-15 minutes of an activation notification
- The goal of the virtual DART meeting is to share updates, answer questions regarding system status (e.g., what is up/what is down), and identify any downstream or upstream impacts of the downtime
- An Initial Downtime Assessment Response Team (iDART) may be activated first as an initial sensing mechanism for the IS AOC to verify if an unplanned downtime is occurring or if it is an isolated event
- If the DART decides there is a wide spread issue, or identifies a potential impact to hospital operations, patient care, or patient safety, this will trigger an activation of the Incident Management Team or (Hospital) Incident Command System

Appendix IV:

Sample Downtime Response Communication Flow

Each unplanned downtime event will have unique complexities, however establishing a trusted, practiced, framework to support communication will mitigate unavoidable impacts.

Process Flow:



Hospital Leadership receives a call but is unsure of the extent of the downtime

IT Leadership receives a call, but is unsure of the extent of the downtime impact

Emergency Preparedness staff receives a call, but is unsure of the extent of the impact

A page is sent to the Initial Downtime Assessment and Response Team (DART)

The iDART communicates within 10 minutes to assess the issues

Concerns identified?

Unsure

Major Concerns

Yes

No

Activate full hospital disaster response

Activate the full Downtime Assessment and Response Team (DART)

- Communicate
- Monitor

Appendix V:

Sample Downtime Response Messaging

iDART assessment page:

iDART activation: please poll end users to assess impact of network slowness. Report to X within 10 minutes.

DART activation page:

DART activation: Network issue impacted lab results. Assess for patient safety and join conference call at 3:30p. 800-123-4567 access: 1234

IMT activation page:

IMT activation: Network issue impacted lab results. Join conference call at 3:30p. 800-123-4567 access: 1234 to develop response plan

Email to staff:

To: All Staff

Subject: ALERT, ALERT, ALERT: Clinical Impact

Dear Colleagues,

Update as of January 23, 4:00pm

As of 3:00p, Server issues have been impacting Lab processing, all technical staff are aware and committed addressing the issue.

All labs requests must be sent according to downtime protocols. Additional instructions, including downtime forms, are available via this link <link.com>.

Please share this update with your staff and colleagues to plan your clinical operations accordingly. We thank everyone for your patience, understanding, and teamwork. We plan to send the next update at 7:00PM unless further communication is warranted sooner.

Sincerely,

Leadership

Appendix VI:

Developing a Downtime Assessment and Response Team

When a downtime event occurs it is critical that key stakeholders meet on a regular basis to brief one another. A well-organized agenda will guide the response group through a concise discussion of the event to rapidly identify key issues and develop a response plan.

Briefing Agenda:

- Identify the response team
  - Representatives from Information Systems
  - Representation from Emergency Preparedness
  - Representatives from critical patient care and operational areas
  - Appropriate level of leadership involvement

- Update from IS subject matter experts
  - Understand the scope of the issue
  - Discuss the cause of the issue
  - Timeframe for resolution

- Evaluate business impact

- Address patient safety concerns
  - Incorporate patient safety representatives and patient safety data into response planning

- Set response objectives
  - Patient census and patient flow
  - Staffing
  - Downtime tools (paper forms, failsafe reports)
  - Planning ahead for reconciliation and recovery

- Communication strategy

- Assign priority tasks to appropriate individuals

- Establish time/place for next briefing

Appendix VII: Sample Downtime Event Status Report

IS DOWNTIME EVENT STATUS REPORT
FOR OFFICIAL USE ONLY - DO NOT DISTRIBUTE

INCIDENT NAME:	**DATE:** **SITUATION REPORT #** Next Status Update Due:

SITUATION SUMMARY:

✓ Identify the response team

✓ Update from IS subject matter experts
- Understand the scope of the issue
- Discuss the cause of the issue
- Timeframe for resolution

✓ Evaluate business impact

✓ Address patient safety concerns

✓ Set response objectives
- Patient census and patient flow
- Staffing
- Downtime tools (paper forms, failsafe reports)
- Planning ahead for reconciliation and recovery

✓ Assign tasks

✓ Establish time/place for next briefing

RESPONSE STAFF:	NAME:	DEPT./EXPERTISE
Incident Leader:		
Emergency Preparedness:		
Documentation Manger:		
Information Systems:		
Department Representation:		

OTHER:

OBJECTIVES/TASKS

DEPT./ INDIVIDUALS:	TASK:	COMPLETE

NEXT MEETING AND/OR CONFERENCE CALL:

DATE: TIME: LOCATION:

PREPARED BY (NAME AND POSITION/TITLE):