# Executive Brief

## Unplanned Downtime of Health Information Technology Systems

**PARTNERSHIP** *for*
**HEALTH IT PATIENT SAFETY**
*Making healthcare safer together*

### Why Is Preparing for Unplanned Downtime Important?

"The more sophisticated the electronics, the less familiarity people have with doing calculations or writing notes on paper, and the harder it's going to be to prepare for and to cover [during a downtime]," explained Ellen Deutsch, MD, medical director of patient safety, risk, and quality, ECRI Institute, to participants at the daylong *Partnership for Health IT Patient Safety* meeting "Partnering for Transformation," held September 16, 2016, at ECRI Institute.

Unplanned system downtime should be treated like any emergency. It will have a significant effect on workflows from registration through discharge. Therefore, the organization should prepare for such an event like it prepares for other emergencies, with backup plans, drills and simulated scenarios, and other proactive risk assessments and tools.
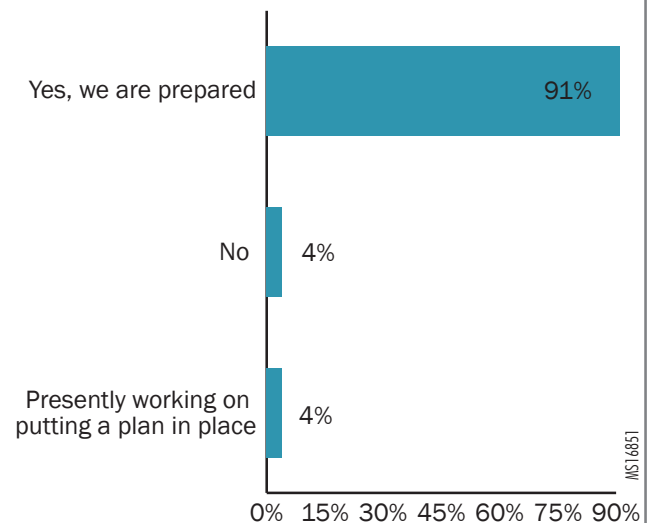
### Did You Ask?

- Is downtime treated like and prepared for like an emergency?
- Do staff receive training and education regarding policies, protocols, and procedures for unplanned health information technology (IT) system downtimes?
- Are unplanned downtimes investigated and debriefed, and are findings and responses shared throughout the organization?

**WHAT PARTICIPANTS ARE SAYING**

When *Partnership* participants were asked about their perceived readiness for unplanned downtime, the vast majority responded that they are prepared for such an event. A small percentage of participants responded either that they are not or that they are developing a plan.

**Figure. Do You Have Practices in Place for an Unanticipated Downtime?**



| Response | Percentage |
|---|---|
| Yes, we are prepared | 91% |
| No | 4% |
| Presently working on putting a plan in place | 4% |

**PARTNERSHIP** *for*
**HEALTH IT PATIENT SAFETY**
*Making healthcare safer together*

# Self-Assessment Questionnaire: Unplanned Downtimes of Health Information Technology Systems

Use this self-assessment questionnaire in conjunction with the following resources to review your unplanned downtime policies and procedures. Then, use the attached action plan template to track resulting projects, initiatives, and reviews.

- ECRI Institute guidance article: Emergency management https://www.ecri.org/components/HRC/Pages/SafSec6.aspx*

- ECRI Institute guidance article: Technology acquisition and management https://www.ecri.org/components/HRC/Pages/MedTech1.aspx*

- Office of the National Coordinator for Health Information Technology (ONC). SAFER guide: contingency planning https://www.healthit.gov/sites/safer/files/guides/safer_contingencyplanning_sg003_form_0.pdf

- U.S. Department of Health and Human Services. Breach notification rule http://www.hhs.gov/hipaa/for-professionals/breach-notification/

## Organization Preparation

| | yes | no | n/a | in progress | notes |
|---|---|---|---|---|---|
| 1. Is an unplanned downtime treated like and prepared for like any other emergency? | ☐ | ☐ | ☐ | ☐ | |
| a. Is consideration of unplanned system downtimes part of the organization's emergency planning and preparation? | ☐ | ☐ | ☐ | ☐ | |
| b. Does leadership support and champion preparation for unplanned system downtimes? | ☐ | ☐ | ☐ | ☐ | |
| c. Is downtime preparation overseen by a multidisciplinary team so that all staff roles are spoken for, understood, and specifically considered? | ☐ | ☐ | ☐ | ☐ | |
| d. Are considerations tailored to specific departments or areas as needed? | ☐ | ☐ | ☐ | ☐ | |
| e. Is there a system in place for appropriate notifications when one area is experiencing an unplanned downtime? | ☐ | ☐ | ☐ | ☐ | |

## Staff Training and Education

| | yes | no | n/a | in progress | notes |
|---|---|---|---|---|---|
| 2. Do staff receive training and education regarding policies, protocols, and procedures for unplanned health information technology (IT) system downtimes? | ☐ | ☐ | ☐ | ☐ | |
| a. Does training and continuing education include regular updates and reviews? | ☐ | ☐ | ☐ | ☐ | |

---

\* Some materials are included in memberships to ECRI Institute products and services. For information about these reports, contact clientservices@ecri.org

| | yes | no | n/a | in progress | notes |
|---|---|---|---|---|---|
| b. Does training and education include items such as ransomware, malware, phishing, and other extraneous disruptions (e.g., items that not only impact the safety but also in the integrity of systems)? | ☐ | ☐ | ☐ | ☐ | |
| c. Are staff members trained in use of paper or alternative system use? | ☐ | ☐ | ☐ | ☐ | |
| d. Are paper or alternative systems and protocols available? | ☐ | ☐ | ☐ | ☐ | |
| e. Does training cover all staff on all shifts, as appropriate, including evenings and weekends? | ☐ | ☐ | ☐ | ☐ | |
| 3. Are simulated downtimes used as ways to prepare for an actual event? | ☐ | ☐ | ☐ | ☐ | |
| a. Are opportunities for simulation training extended to staff on all shifts and in all departments? | ☐ | ☐ | ☐ | ☐ | |
| b. Does debriefing after simulation training occur? | ☐ | ☐ | ☐ | ☐ | |
| c. Are changes to downtime policies, procedures, and protocols made as a result of concerns identified during simulation training? | ☐ | ☐ | ☐ | ☐ | |
| 4. Does debriefing occur after downtime incidents to identify issues that should be addressed in future training or in amendments to policies? | ☐ | ☐ | ☐ | ☐ | |
| a. Are changes to downtime policies, procedures, and protocols made as a result of concerns identified during unplanned downtimes? | ☐ | ☐ | ☐ | ☐ | |
| b. Do preparations for downtimes include preparations and protocols for such times as when staff levels are at their lowest, such as overnight, on weekends, and on holidays? | ☐ | ☐ | ☐ | ☐ | |
| c. Are tools, such as the SAFER guides, used to measure an organization's preparedness for unplanned system downtimes? | ☐ | ☐ | ☐ | ☐ | |

## Backup Systems and Equipment

| | yes | no | n/a | in progress | notes |
|---|---|---|---|---|---|
| 5. Are unplanned downtime policies, procedures, and protocols available for reference in a location and format that is accessible during an unplanned system downtime? | ☐ | ☐ | ☐ | ☐ | |
| a. Do staff know where items are located and how to access them when needed? | ☐ | ☐ | ☐ | ☐ | |
| b. Is the location of materials in a place that is convenient and known to all staff? | ☐ | ☐ | ☐ | ☐ | |

**PARTNERSHIP** *for*
**HEALTH IT PATIENT SAFETY**
*Making healthcare safer together*

|  | yes | no | n/a | in progress | notes |
|---|---|---|---|---|---|
| c. Is there someone available within the organization at all times who has access to this location? | ☐ | ☐ | ☐ | ☐ | |
| d. Is the content and location of available materials standardized across the organization? | ☐ | ☐ | ☐ | ☐ | |
| 6. Is there a tool box with available tools, forms, and other backup items needed for periods of unplanned downtimes? | ☐ | ☐ | ☐ | ☐ | |
| a. Do staff know where these tools and items are located? | ☐ | ☐ | ☐ | ☐ | |
| b. Do staff know how to use these tools and materials and how information will be re-incorporated into the record? | ☐ | ☐ | ☐ | ☐ | |
| c. Are these tools and items easily accessible? | ☐ | ☐ | ☐ | ☐ | |
| d. Are there sufficient supplies for all staff who may be working when the system goes down? | ☐ | ☐ | ☐ | ☐ | |
| e. Are these backup items regularly assessed for appropriateness, efficacy, and usability? | ☐ | ☐ | ☐ | ☐ | |
| f. Are batteries or backups regularly tested or replaced? | ☐ | ☐ | ☐ | ☐ | |
| g. Is the location and content of such tool boxes standardized? | ☐ | ☐ | ☐ | ☐ | |
| 7. Do forms meant for use during system downtime match the system they're replacing as closely as possible? | ☐ | ☐ | ☐ | ☐ | |
| 8. Are staff roles during unplanned downtimes clearly defined? | ☐ | ☐ | ☐ | ☐ | |
| a. Are staff aware of their roles during unplanned downtimes? | ☐ | ☐ | ☐ | ☐ | |
| b. In the acute care setting, are certain staff members designated as "runners" for pharmacy, blood bank, laboratory, and other departments? | ☐ | ☐ | ☐ | ☐ | |
| c. Do non-critical providers have designated supporting roles during downtimes? | ☐ | ☐ | ☐ | ☐ | |
| d. Are these roles reviewed regularly for accuracy and appropriateness? | ☐ | ☐ | ☐ | ☐ | |
| e. Is a list of these roles included with the reference documents and tool box? | ☐ | ☐ | ☐ | ☐ | |

## Communication and Notification

| | yes | no | n/a | in progress | notes |
|---|---|---|---|---|---|
| 9. Are "command center" principles used to manage unplanned downtimes? | ☐ | ☐ | ☐ | ☐ | |

| | yes | no | n/a | in progress | notes |
|---|---|---|---|---|---|
| **10.** Is there a rapid notification system in place to inform staff (including those in IT) of unplanned system downtimes and disruptions, and alerting staff to what systems are impacted? | ☐ | ☐ | ☐ | ☐ | |
| a. Is this notification system tested regularly? | ☐ | ☐ | ☐ | ☐ | |
| b. In the acute care setting, are staff in all departments who might be affected by downtime notified, even if the downtime occurs in a separate department (e.g., if a lab system goes down, are staff in the emergency department, intensive care unit, and others notified)? | ☐ | ☐ | ☐ | ☐ | |
| **11.** Are appropriate forms and notifications in place to inform all stakeholders of the downtime (e.g., in the event of a ransomware breach)? | ☐ | ☐ | ☐ | ☐ | |
| a. Does this notification include which system is down and which are impacted? | ☐ | ☐ | ☐ | ☐ | |
| b. Does this notification include which areas are directly and indirectly affected? | ☐ | ☐ | ☐ | ☐ | |
| c. Does this notification include an estimate, if at all possible, of when the system will be restored? | ☐ | ☐ | ☐ | ☐ | |
| d. Does this notification include information on what actions should be taken in the meantime? | ☐ | ☐ | ☐ | ☐ | |
| e. Are staff designated to speak with the media when appropriate? | ☐ | ☐ | ☐ | ☐ | |
| f. Are these staff provided with talking points and resources for additional information? | ☐ | ☐ | ☐ | ☐ | |
| g. Are other staff trained to refer all inquiries to the appropriate designated staff? | ☐ | ☐ | ☐ | ☐ | |
| h. If a breach is involved, are the assessment, notification, and disclosure steps taken, as required by regulations (i.e., HIPAA [Health Insurance Portability and Accountability Act] and privacy and security rules)? | ☐ | ☐ | ☐ | ☐ | |
| i. Is a staff member designated and authorized to coordinate assessments and disclosures? | ☐ | ☐ | ☐ | ☐ | |
| j. Does this staff member communicate with the media when appropriate? | ☐ | ☐ | ☐ | ☐ | |
| k. Are all staff members and those impacted (e.g., including those whose information may have been compromised) promptly informed of the breach? | ☐ | ☐ | ☐ | ☐ | |
| l. Is the extent of the breach disclosed as it is identified? | ☐ | ☐ | ☐ | ☐ | |

| | yes | no | n/a | in progress | notes |
|---|---|---|---|---|---|

## Recovery

12. Is a method in place to inform staff when the system has safely come back online?  ☐ ☐ ☐ ☐

13. Is a procedure in place for synchronizing information recorded via backup methods when the health IT system is restored?  ☐ ☐ ☐ ☐

   a. Is a procedure in place to ensure that data entered via backup system is transcribed or scanned into the primary system?  ☐ ☐ ☐ ☐

   b. Are the effectiveness, accuracy, and safety of this procedure ensured?  ☐ ☐ ☐ ☐

   c. Is any data lost made known to the risk manager or designated staff member and documented appropriately in the primary system?  ☐ ☐ ☐ ☐

   d. Is the loss of data investigated and origins of the loss reviewed?  ☐ ☐ ☐ ☐

   e. Does the electronic health record (EHR) allow postadministration documentation with distinct "time of entry" and "time of administration" entries?  ☐ ☐ ☐ ☐

14. Is a procedure in place for the safe handling, receipt, and incorporation of any hardcopy information generated during system unplanned downtimes?  ☐ ☐ ☐ ☐

15. Is a method in place to ensure that billing for care provided during unplanned system downtimes can be managed and documented?  ☐ ☐ ☐ ☐

## Investigation

16. Are unplanned downtimes investigated?  ☐ ☐ ☐ ☐

17. Are findings about unplanned downtimes shared throughout the organization?  ☐ ☐ ☐ ☐

# Action Plan
## Unplanned Downtime of Health Information Technology Systems

**Assessment completed by:** _____     **Date:** _____

| QUESTION NO. | ACTION REQUIRED | RESPONSIBILITY | TARGET DATE | ACTION COMPLETED | |
|---|---|---|---|---|---|
| | | | | DATE | INITIALS |
| | | | | | |