

Health Care Facility-Level Downtime Assessment

Introduction

This Health Care Facility-Level Extended Downtime Assessment is a voluntary tool designed to help individual health care facilities evaluate their current state of downtime readiness and identify gaps, promising practices, and current policies. It can also serve as a tool to guide discussions; develop surveys; identify promising practices; and outline areas for education, engagement, and support. Health care coalitions (HCC) may also use this tool to engage members for the HCC Extended Downtime Impact Assessment. This assessment is not mandatory for health care facilities or HCCs; it is intended to support internal or jurisdictional planning. Note that this tool also considers utility failures as a form of downtime to promote broader discussions with the HCC about operational redundancy and potential gaps.

The information collected through this assessment can be highly sensitive. To protect the security and operational integrity of participating facilities, any data submitted to or shared with HCCs should be fully de-identified before dissemination. For example, instead of asking for the facility name, HCCs should request only the facility type. This aligns with existing guidance that sensitive information generated through assessments should be deidentified prior to sharing or being used in broader planning efforts.

While this document can be used to support the HCC-level cybersecurity preparedness efforts, it is focused solely on activities, systems, and processes within the facility itself. Results should be used to inform cybersecurity and extended downtime planning, strengthen resilience to cyber and utilities failures and support safe continuation of care during system disruptions. This tool is not intended for regulatory purposes or oversight purposes of health care facilities, comparison between facilities, or scoring. It is designed to promote candid evaluation and facilitate data-driven internal improvements.

Use the [Health Care Facility-Level Cybersecurity Assessment](#) to evaluate the current state of cybersecurity resilience in your facility.

Use the [HCC Extended Downtime Health Care Delivery Impact Assessment](#) to evaluate HCC downtime readiness across their jurisdictions. It supports identifying gaps, promising practices, and existing policies at the HCC level.

Access the [Cybersecurity Resource Page](#) for related plans, tools, and templates.

The [Utility Failures in Health Care Toolkit](#) can strengthen facility preparedness for utility failures.

Completion of this assessment may require coordination among clinical, technical, administrative, and emergency management personnel within the facility. As noted in related HCC-level tools, assessment leads may find it helpful to engage a multidisciplinary working group to ensure accurate and comprehensive responses.

Assessment Process

Each health care system and/or facility participating in the assessment should identify a lead assessor. Every facility should report its results, regardless of whether it is part of a corporate system. The lead assessor will serve as the primary point of contact, coordinate input from multiple disciplines, and may establish a working group to support ongoing activities. Because many responses are facility-specific, multi-hospital systems may choose to complete separate assessments for each facility or document differences within a single consolidated report. If results are shared with the HCC, facility names should be redacted.

For each function, the activity should be acknowledged as being implemented using a “yes,” “no,” or “partial” answer. Facilities may use the “Notes” column to provide additional context or explanations. If an HCC uses this assessment to create a survey for its members, the “Notes” column may be omitted. In all cases, sensitive or identifying information should be removed from the “Notes” column prior to circulating the survey outside of the facility/system.

Given the sensitivity of the information that may be collected, the health care system/facility can choose to handle and utilize the data in a manner agreed upon by the partners, such as:

- Submitting de-identified data to the HCC.
- Submitting de-identified responses to select questions to highlight the most significant gaps identified by the facility/health system, especially those relevant to regional planning and HCC activities.
- Participating in HCC-mediated discussion sessions to identify key areas of concern and potential best practices.

This approach helps enhance internal awareness of issues, fosters a common understanding of mitigation and preparedness efforts, and assists the HCC and the participant in identifying key focus areas for training, engaging subject matter experts, sharing best practices, and conducting exercises in subsequent years.

Related ASPR TRACIE Resources

- [Health Care Cybersecurity Resources Page](#)
- [Cybersecurity Topic Collection](#)
- [Electronic Health Records and Downtime Procedures Topic Collection](#)
- [HCC Cybersecurity Assessment](#)
- [HCC Extended Downtime Health Care Delivery Impact Assessment](#)
- [Health Care Facility-Level Cybersecurity Assessment](#)
- [Healthcare System Cybersecurity: Readiness & Response Considerations](#)
- [Utility Failures in Health Care Toolkit](#)
- [Utility Failures Topic Collection](#)

Additional Related Resources

- [ASPR's Office for Cybersecurity and Infrastructure Protection Bulletins](#)
- [CISA: National Cyber Awareness System-Bulletins, Alerts Subscription, Cybersecurity Services and Tools, Infrastructure Resilience Planning Framework Playbook, and Tabletop Exercise Packages](#)
- [FEMA Healthcare Facilities and Power Outages: Guidance for State, Local, Tribal, Territorial, and Private Sector Partners](#)
- [Health Sector Coordinating Council Cybersecurity Working Group](#)
- [HHS 405\(d\)](#)
- [HHS Cyber Gateway](#)
- [HHS emPOWER Program](#)
- [NIST Cybersecurity Framework \(CSF\) 2.0](#)

Acknowledgements

Contributors and reviewers of this document are listed alphabetically and include: **David Csernak**, MSHA, MA, Regional Supervisor (Acting), Office of Health Care Readiness, HHS ASPR; **Craig DeAtley**, PA-C, Director, Institute for Public Health Emergency Readiness, MedStar Washington Hospital Center; **Garrett Hagood**, Director of Special Initiatives, CISO, Coastal Bend Regional Advisory Council; **John Hick**, MD, ASPR TRACIE and Hennepin Healthcare; **Jodi Keller**, RN, Director of Healthcare System Emergency Preparedness and Response/ Central Region Healthcare Coordinator, COTS; **Mary Russell**, EdD, MSN, Healthcare Emergency Response Coalition, Palm Beach County, FL; **Robin Oothoudt**, HcEM, RS, Executive Director, Arizona Coalition for Healthcare Emergency Response; and **Lori Upton**, Chief Executive Officer, SouthEast Texas Regional Advisory Council.

Health Care Facility-Level Extended Downtime Assessment

The following inquiries are specific to downtime-related activities within individual health care delivery systems (e.g., hospitals or similar facilities). Participation is voluntary, and not all questions may apply depending on the facility size and complexity. The designated point of contact should complete the assessment with input from relevant internal partners. Responses may represent the entire health care system, a single facility, or a combination when capabilities vary across facilities.

Facility-Level Extended Downtime Activity	Yes/ No/ Partial/ NA	Additional Notes
1. General Downtime Practices		
1.1. Does the facility or system have defined thresholds for activating downtime processes (e.g., expected duration of more than two hours)?		
1.1.1. Is there a process to identify who is authorized to activate downtime procedures and does this vary by affected system?		
1.1.2. Is there a mechanism in place to communicate the activation decision to line employees when normal communication channels may be down?		
1.1.3. Is there a plan for messaging to: <ul style="list-style-type: none"> • Staff • Patients • Regulatory agencies • Public 		
1.2. Is there a downtime “playbook” that maps initial actions and defines roles and responsibilities, and is it available in print and on portable storage devices (e.g., USB, shared offline folder)?		
1.2.1. Is there a defined decision matrix, specifying the criteria and individuals authorized to make decisions, for transitioning to clinical downtime procedures?		
1.3. Have leaders and clinical and support staff (e.g., lab, pharmacy) been trained in extended downtime processes?		
1.3.1. Are roles and responsibilities clear?		



Facility-Level Extended Downtime Activity	Yes/ No/ Partial/ NA	Additional Notes
1.3.2. Is there a template for Hospital Incident Command structure and functions for a downtime event (e.g., branches for the information technology [IT] vs. clinical response and who will lead each)?		
1.3.3. Are adequate resources available on the units for employee reference and downtime documentation (e.g., paper forms, portable storage media, clipboard, pens)?		
1.3.4. Are just-in-time downtime procedure training resources available for clinical and support services (e.g., lab and pharmacy)?		
1.3.5. Are informatics or other subject matter experts available to support and guide implementation of downtime procedures?		
1.3.6. Are the plans and processes exercised/drilled regularly?		
1.3.7. Is there a process to determine if other facilities in the region are affected?		
1.4. Are hard copies of internal and external contact lists (e.g., notification lists, on-call lists) current and accessible?		
1.5. Are staff schedules and on-call lists and calendars stored locally on computers or drives that are insulated from the network or is there a defined process to recreate them if needed?		
1.6. Does the facility or system have a downtime communication and information sharing plan that includes multiple modalities (traditional/non-traditional, primary/backup)?		
1.6.1. Is there a process to notify leadership and external partners (including Emergency Medical Services [EMS]) providers when cyber incidents or downtime events may result in diversion or impact EMS communications/systems?		
1.7. Is there a process to assess and minimize the impact of extended downtime on supply chains, including the following ordering and delivery needs: <ul style="list-style-type: none"> • Medical supplies 		



Facility-Level Extended Downtime Activity	Yes/ No/ Partial/ NA	Additional Notes
<ul style="list-style-type: none"> • Blood products • Oxygen/medical gases • Pharmaceuticals • PPE • Medical devices (e.g., ventilators) • Food/beverage • Support services (e.g., laundry, cleaning) • Water 		
<p>1.8. Are plans in place for obtaining additional staffing needed during downtime, including:</p> <ul style="list-style-type: none"> • Clinical and administrative personnel • Cyber/IT experts • Utility specialists • Runners /scribes 		
<p>1.8.1. Is there an initial template (e.g. additional staffing guide with priority for intensive care unit, emergency department, labor and delivery, and others) to guide early resource allocation?</p>		
<p>1.9. During downtime activation, is there a process to work with providers and nursing staff to estimate patient care impacts and identify and implement alternatives?</p>		
<p>1.10. Is there a system to report and monitor adverse safety events and near-misses during downtime?</p>		
<p>1.11. Does the downtime plan address heating, ventilation, and air conditioning (HVAC) IT control systems?</p>		
<p>1.12. Does the plan address limiting, adjusting, and re-prioritizing inpatient and outpatient services?</p>		
<p>1.13. Does the plan address patient transfer and/or evacuation coordination during IT or utilities failure?</p>		



Facility-Level Extended Downtime Activity	Yes/ No/ Partial/ NA	Additional Notes
1.13.1. Are there predefined triggers for initiating patient diversion, transfer, or evacuation during prolonged downtime or utility failure?		
1.14. Does the plan include managing large volumes of paper charts and documents during downtime?		
1.14.1. Does this include scanning, filing system, secure storage, and staff hours for these tasks?		
1.15. Are adequate resources available to support paper-based processes (e.g., printers, copiers, paper, toner)?		
1.15.1. Are downtime forms and procedures pre-printed for a specific time limit (e.g., 48 hours of forms)?		
1.15.2. Are these forms regularly reviewed for necessary updates?		
1.15.3. Are local printing services or contract providers available to reproduce legacy paper forms on short notice (e.g., atypical sizes, carbon copies)?		
1.16. Does the downtime plan include alternate methods for: <ul style="list-style-type: none"> • Patient triage and registration • Submitting clinical orders • Obtaining and communicating test and diagnostic results (including urgent) • Managing drug dispensing systems manually • Tracking medication and supply use for replenishment/ordering during extended downtime • Rapid credentialing • Security/badge access • Scheduling patients and staff • Timesheets and payroll • Cafeteria, gift shop, and parking payments 		



Facility-Level Extended Downtime Activity	Yes/ No/ Partial/ NA	Additional Notes
1.17. Does the plan address how to manage accounts receivable/ payable, external ordering, and any third-party attestations required before restoring connectivity?		
1.18. Do employees understand how to access backup data if electrical or IT systems are down?		
1.19. Are alternate resources available to replace electronic medical reference materials during utility failure or IT disruptions (e.g., dosage tables, cardiac arrest management algorithms)?		
1.20. Does the plan include processes for safely restoring data and services and for staged reconciliation and recovery of paper documentation as systems are restored?		
2. IT System/Network Downtime		
2.1. Are alternate IT and telecommunication plans in place for cyber incidents, including paging, phones, Wi-Fi, and internet failure (including use of cellular, satellite, and other technology)?		
2.2. Does the plan identify alternatives for critical technology-dependent services that could be disrupted and adversely impacted during a cyber incident including: <ul style="list-style-type: none"> • Patient care and safety monitoring systems • Access controls to certain areas (e.g., pediatrics, labor and delivery, psychiatry) • Remote chart access/utilization • Patient registration/discharge • Documenting patient care bedside charges • Telemedicine • Overhead paging • Pager utilization • Emergency messaging 		
2.3. Does the plan specify how existing electronic medical records will be accessed?		



Facility-Level Extended Downtime Activity	Yes/ No/ Partial/ NA	Additional Notes
2.3.1. Is there a “hotline” or alternative method for obtaining access from a different location that has internet/other services?		
2.4. Are critical contacts, networks, and partners documented and accessible during a cyber incident?		
3. Electrical Failure		
3.1. Does the facility maintain electrical failure downtime plans that address key clinical and support functions (e.g., HVAC)?		
3.1.1. Are average and peak power consumption requirements known to inform backup power needs?		
3.2. Are uninterruptable power supplies available for critical systems/devices, with an inventory, maintenance program, and reserve supply?		
3.3. Does the generator and backup power plan address: <ul style="list-style-type: none"> • Maintenance and suitability for prolonged use • Redundancy (more than one generator) • Agreements with electricians for mobile generator connections, leasing/obtaining external generators and required capacity (e.g., kW capacity, delivery and connection time) • Cable/wiring harness connectivity needs and lengths to external unit location(s) • Protection of generators and transfer switches from external threats (e.g., flooding) • Staff training on emergency procedures 		
3.4. Does the plan address utility failure promising practices such as: <ul style="list-style-type: none"> • Turning off (and unplugging) unused equipment to conserve power and prevent potential power surge damage upon restoration • Maintaining power to fire alarms and fire suppression systems • Having an emergency lighting plan in case of generator failure, to include distribution of supplies and battery back-up for key lights 		



Facility-Level Extended Downtime Activity	Yes/ No/ Partial/ NA	Additional Notes
<ul style="list-style-type: none"> Ensuring backup power supplies for access/egress controls (e.g., doors, card readers, garage doors) are considered Restricting elevator use when on generator power 		
3.5. Is there a mechanism to address direct monitoring of patients if remote telemetry/video monitoring fails?		
3.5.1. Are alternative monitoring methods planned?		
3.5.2. Is there a plan for how staff will be supplemented to ensure adequate monitoring?		
3.6. Can key services requiring significant energy (e.g., laundry, food) be outsourced during electrical failure?		
3.7. Are personnel trained in life-safety needs during complete power failure (e.g., monitoring ventilator and other device batteries, bagging patients, running gravity drips, transitioning to tank oxygen if necessary)?		
3.7.1. Are related paper checklists available to support staff and providers during complete power failure?		
3.8. Does the backup power plan address equipment that is not linked to backup power and may require additional personnel/monitoring (e.g., patient call buttons, emergency buttons)?		
3.9. Does the plan address pharmaceutical, lab, diagnostic, and electronic health record needs?		
3.10. Does the backup power allow HVAC operation, or are alternate climate control measures included?		



Facility-Level Extended Downtime Activity	Yes/ No/ Partial/ NA	Additional Notes
3.10.1. Are areas requiring specific temperature /humidity controls identified (e.g., surgical and sterile areas, server rooms, radiology)?		
3.10.2. Are emergency stock supplies available for heating/cooling needs (e.g., blankets, additional ice machines)?		
3.10.3. Does the facility have onsite extra fuel storage and related documentation/plans (e.g., quantity, location, vulnerability, ability to use alternative fuels, and the time required to transition systems to full load capacity)?		
3.11. Are procedures for temperature-sensitive perishables (e.g., food, pharmaceuticals, lab) addressed?		
3.12. Is there an emergency downtime feeding plan for patients and staff that accounts for dietary restrictions?		
4. Water and Sewer		
4.1. Does the facility/system maintain a water disruption plan, to include the following considerations: <ul style="list-style-type: none"> • Usage analysis (potable and service) • A list of commercial water vendors and relevant inventory (e.g. tanker truck vs. bottled drinking water, five-gallon jugs) • Identify locations of main water service lines and determine if they are co-located with other utilities • Number of and location water service connections to the facility • Determine if each service connection can support the full facility load independently 		
4.2. Is a temporary supply of potable water immediately accessible?		
4.3. Does the downtime plan include water conservation measures?		



Facility-Level Extended Downtime Activity	Yes/ No/ Partial/ NA	Additional Notes
4.4. Are purified or specialty treated water needs per patient identified for normal versus modified operations?		
4.5. Is there a plan for water distribution within the facility during utility failure (potable and non-potable, food preparation, dialysis)?		
4.6. Is there a plan for testing, purging, and disinfecting water systems in case of contamination?		
4.7. Does the plan address fire suppression needs including preplanning with local fire departments, pressure needs, and connections?		
4.8. Are trained fire watch personnel available during extended outages?		
4.9. Does the plan address impacts, such as: <ul style="list-style-type: none"> • Contamination of municipal supply (e.g., boil water orders) • Loss of pressure from municipal supply (including complete and partial) • Loss of sewer capacity (e.g., drains/toilets not functional) 		
4.10. Are check valves regularly maintained to prevent reflux of water or sewage into the facility?		
4.11. Is there an external water supply plan (e.g., “dairy line” to tanker, bladder, on-site well)?		
4.11.1. Are contracts in place with vendors that will prioritize hospital water delivery?		
4.11.2. Is there a plan for monitoring external supplied water for potential bacterial contamination?		
4.12. Are outsourcing plans in place for water-reliant services (e.g., laundry, food, cleaning)?		
4.13. Does the plan address hand hygiene and infection control needs during water shortages?		



Facility-Level Extended Downtime Activity	Yes/ No/ Partial/ NA	Additional Notes
4.14. Is there a plan for monitoring and reporting environmental care issues (e.g., leaks, slippery floors, mold)?		
4.15. Are prioritized contracts in place for remediation companies for the following needs: <ul style="list-style-type: none">• Electrical• Mechanical• Structural• Specialized		

