Health Care Facility-Level Cybersecurity Assessment

Introduction

This Health Care Facility-Level Cybersecurity Assessment is a voluntary tool designed to help individual health care facilities evaluate their current cybersecurity posture, identify vulnerabilities, and highlight strengths in preparedness and response capabilities. 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 Cybersecurity Assessment. This assessment is not mandatory for health care facilities or HCCs; it is intended to support internal or jurisdictional planning.

Use the **Health Care Facility-Level Extended Downtime Assessment** to evaluate downtime readiness within your facility.

Use the **Health Care Coalition (HCC) Cybersecurity Assessment** to evaluate the current state of cybersecurity resilience **within HCCs.** 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 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 de-identified prior to sharing or being used in broader planning efforts.

While this document can support HCC-level cybersecurity preparedness efforts, its primary focus is on activities, systems, and processes within individual facilities. The results should be used to guide cybersecurity planning, enhance resilience, and support safe continuity of care during cyber disruptions at the facility level, where tactical decisions can be implemented. 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.

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 over time.

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 Extended Downtime Assessment
- Healthcare System Cybersecurity: Readiness & Response Considerations

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
- Health Sector Coordinating Council Cybersecurity Working Group
- HHS 405(d)
- HHS Cyber Gateway
- 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 L. 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 Cybersecurity Assessment

The following inquiries focus on cybersecurity-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 size and complexity of the cyber infrastructure. 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 Cyber Activity	Yes/No/ Partial/NA	Additional Notes
1. Cyber Hygiene and Preparedness		
1.1. Does the facility use any or all these cybersecurity practices to protect data/system infrastructure? • Network segmentation • Redundancy • Centralized log collection • Configuration management		
1.2. Do cyber hygiene practices incorporate the following as outlined in the HPH Cybersecurity Performance Goals (CPGs)? • Email security/ encryption • Multifactor authentication • Access management (badging, credential revocation, separate user/admin accounts)		
1.3. Do cybersecurity planning efforts (e.g., external vendor, device, system, or software vulnerabilities) consider third-party vulnerabilities?		
1.4. Have measures been implemented to ensure servers and other hardware are protected from utility failures, environmental threats (e.g., flooding), and other risks?		

Facility-Level Cyber Activity	Yes/No/ Partial/NA	Additional Notes
1.5. Are defenses in place to protect against denial-of-service attacks that could affect phones, internet sites, and 911 systems?		
1.5.1. Does the facility maintain non-networked backup communication systems (e.g., satellite phones) for use during cyber incidents?		
1.6. Does the facility or system conduct cybersecurity training or exercises (e.g., downtime, cyber hygiene)?		
1.6.1. Are personnel trained to recognize and report potential issues related to a cyber incident?		
1.6.2. Are test phishing emails sent to evaluate staff recognition and reporting, and if users do not pass, is there a remediation plan for the user?		
1.7. Is there a facility or system work group or committee dedicated to cyber initiatives and issues?		
1.7.1. Are recent cyber threats monitored/reviewed to maintain situational awareness?		
1.7.2. Is an After Action Report (AAR) completed and is a Corrective Improvement Plan (CIP) developed to address and remediate identified issues after an event or in response to identified threats?		
1.7.3. Is threat information communicated to leadership and line staff when appropriate?		
1.8. Are dedicated personnel available to support ongoing/extended cybersecurity preparedness activities (e.g., a cyber subject matter expert/technical expert)?		
1.8.1. If not, are external resources accessible for guidance/support?		
2. Cyber Vulnerabilities		

Facility-Level Cyber Activity	Yes/No/ Partial/NA	Additional Notes
2.1. Has the facility/system conducted an internal evaluation of systems to identify critical vulnerabilities?		
2.2. Does the facility/system conduct vulnerability testing (penetration testing/attack simulations) of key systems?		
2.3. Has a network map/plan been created that shows how software and systems are connected, and how they would be affected during cascading failures?		
2.3.1. Does the map/plan identify safe disconnect points that can be used to isolate unaffected segments during a cyber incident?		
2.3.2. Does the map/plan prioritize systems for protection and restoration based on functionality?		
2.3.3. Does mapping consider how usually integrated software could be used independently to restore some functionality (e.g., hospitals may be able to use laboratory result reporting systems independent of the health record)?		
2.4. Are backup systems defined for each element of vulnerability?		
2.4.1. Is there a policy to ensure backups are not corrupted during and after normal backup processes?		
2.4.2. Do systems have integrated backup/mirroring/redundancy?		
2.4.3. Do systems have warm or hot offsite failover capabilities?		
2.4.4. Do systems have a way to access backups during a system failure?		
2.4.5. Is backup hardware clearly labeled?		

Facility-Level Cyber Activity	Yes/No/ Partial/NA	Additional Notes
3. Cyber Incident Response		
3.1. Does the facility/system have a process to identify a cyber-attack or systems failure and shut down affected systems?		
3.2. Are there criteria to identify those with the authority to shut down systems?		
3.2.1. Is there protocol for who can declare a cyber incident has occurred and activate an Incident Management Team if applicable?		
3.3. Does the facility/system have a cyber / IT systems incident response plan (including a reporting/alerting protocol)?		
3.4. Does the facility/system have a cyber incident communication plan?		
3.4.1. Does it address cyber incident messaging (who to contact, what mechanisms to use when usual systems may be compromised)?		
3.4.2. Are all downtimes communicated to the executive level (e.g., administrator on-call) immediately?		
3.4.3. Does it specify what communications may require approvals and by whom/when (versus what may be performed immediately)?		
3.4.4. Does it address when line personnel should move to downtime procedures?		
3.5. Does the cyber incident plan include an impact-on-services analysis for each system to help IT and executive leaders understand direct and cascading effects on operations?		
3.5.1. Is there a documented priority matrix for system restoration that outlines which systems must be restored first based on operational and clinical needs (e.g., Identity and Access Management before other federated systems, electronic health record tiered above ancillary systems)?		

Facility-Level Cyber Activity	Yes/No/ Partial/NA	Additional Notes
3.5.2. Do these mechanisms address direct monitoring of patients in case of remote monitoring systems failure?		
3.6. Are “clean” computers/tablets that are isolated from networks and software upgrades available for use in case a cyber incident renders current computers unusable?		
3.6.1. Does the plan account for supporting the needs of remote workers?		
3.7. Are mechanisms in place to address physical security in the facility during a cyber incident (e.g., maintaining access control to closed areas of the hospital such as maternity wards or secure medication cabinets)?		
3.8. Are the following legal considerations regularly assessed to optimize protection and reduce risk in case of a cyber incident? • Cyber insurance • Liability waivers • Official internal health care system policies • Third party policies • Ransom policies • Vendor attestation requirements to resume connectivity		
3.9. Is there a plan to segregate the coordination of any criminal/ransom-related activities from the rest of the incident command functions?		
3.9.1. Are there criteria that determine when external partners or law enforcement should be notified during a cyber incident and how to identify who is responsible for coordinating those notifications?		
3.9.2. Are additional agencies/law enforcement organizations identified for inclusion in case of known or suspected criminal action (e.g., FBI, CISA)?		