Health Care Coalition Cybersecurity Assessment

Introduction

Cybersecurity threats and their subsequent impacts on patient care, general safety, and operations have become a near-daily reality for health care coalitions (HCCs), facilities, and practitioners. While modern Health Information Technology (Health IT) provides critical lifesaving functions, reliance on connected networks and systems, wireless technology, and digital health records have left health facilities and systems vulnerable. Recent highly publicized ransomware attacks on hospitals have shown devastating and sometimes long-term impacts that these incidents can have on even well-protected IT systems.

Use the **HCC Extended Downtime Health Care Delivery Impact Assessment** alongside this assessment to help HCCs evaluate **downtime readiness** across their jurisdictions. It supports identifying gaps, promising practices, and existing policies at the HCC level.

Access the **Health Care Coalition Resource Page** for related plans, tools, and templates.

Increasing reliance on health care systems' (HCS) technology coupled with the growing sophistication and prevalence of cyberattacks has made investments in cybersecurity and cyber resilience a top priority. The U.S. Department of Health and Human Services (HHS) Administration for Strategic Preparedness and Response's (ASPR) Hospital Preparedness Program (HPP) recognizes that effective cybersecurity measures require commitment and coordination of numerous entities across the public and private sectors to include hospitals, IT vendors, connected medical device manufacturers, and various levels of government. HHS and the Healthcare and Public Health (HPH) sector are collaborating to accomplish these goals under the current HPP cooperative agreement.

The HHS HPH Cybersecurity Performance Goals (CPGs) help health care organizations prioritize implementation of high-impact cybersecurity practices. These CPGs are voluntary cybersecurity practices that health care organizations, and health care delivery organizations in particular, can prioritize to strengthen cyber preparedness, improve cyber resiliency, and ultimately protect patient health information and safety. They were built off the framework of Cybersecurity and Infrastructure Security Agency (CISA) cross-sector CPGs and informed by common industry cybersecurity frameworks, guidelines, best practices, and strategies. These goals help health care organizations prioritize implementation of high-impact cybersecurity practices and are designed to protect the

health care infrastructure from cyberattacks, improve response when events occur, and minimize residual risk. HCCs may also be affected by cyberattacks and in some cases, can support HCS and individual facilities to assess cybersecurity practices by using the HPH CPGs.[1]

Purpose and Scope

This assessment can help HCCs evaluate the current state of cybersecurity resilience in their jurisdiction and identify gaps, promising practices, and current policies at the coalition level. Note that this assessment is designed for the HCC and coordination level, and *not* the facility/delivery level. As part of the current HPP cooperative agreement, HCCs are expected to complete a Cybersecurity Assessment for their organization, focusing on coalition-level preparedness and response functions. This template can be used to evaluate key areas for cyber resilience planning. *While this assessment can be used to meet that requirement, it is not mandatory to use this template.*

Objectives

This assessment is designed to help identify priority areas for HCC systems and operations to reduce risk and improve overall cyber readiness to maintain HCC operations or support affected members. It is not intended to be used to compare HCCs, "score" an HCC, or be used for regulatory or other administrative purposes. It is designed to allow maximum transparency of key issues while protecting sensitive information. HCC leadership can use the results of this assessment to inform future cybersecurity support needs, including preparedness and response planning between and among coalition members.

The objectives of the assessment are to:

- ✓ Assess use of cybersecurity practices
- ✓ Describe community impact
- ✓ Identify potential mitigation strategies
- ✓ Support current cyber practices
- ✓ Understand and define the role of the HCC during a cyber event

Assessment Process

This assessment focuses on the evaluation of cybersecurity preparedness activities at the *coalition level*. HCCs should identify a lead assessor to complete this section of the

[1] For example: Healthcare Industry Cybersecurity Practices, National Institute of Standards and Technology (NIST) Cybersecurity Framework, Healthcare and Public Health Sector Cybersecurity Framework Implementation Guide

questionnaire and serve as the main point of contact. They will likely need to engage with multiple other individuals to determine accurate responses and may wish to create a workgroup for ongoing activities.

Assessors should provide an answer for each question, based on an approximation of the overall perceived level of completion, from the perspective of **HCC functions and activities** ("yes," "no," "partial," "not applicable"). HCCs vary significantly in their physical and virtual systems, so some questions may not apply to certain coalitions. Assessors should note these omissions by indicating "not applicable" in response to the question/domain that does not apply to their operations. Additional details for each question may be added to the "Notes" column. Including multiple agencies, facilities, and disciplines is recommended to evaluate current cyber preparedness. Sensitive information from the assessment should be deidentified before sharing assessment results.

Assumptions

This document assumes the individual completing the assessment has:

- General understanding of cybersecurity initiatives relevant to the coalition. This includes awareness of previous cyber incidents, evolving cyber threats, and vulnerabilities.
- Basic understanding of the cybersecurity practices already being implemented within the HCC and within the health care delivery systems that make up the coalition.
- Already been exposed to, or is aware of, critical health care cybersecurity principles and practices being referenced in this assessment. This includes any major HPH guidance materials, federal cybersecurity reference documents, or industry best practices.
- Knowledge (or the ability to engage partners that have such knowledge) of the basic health care-related cybersecurity best practices being utilized at the HCC level as well as at the member level.
- General knowledge of the HPH Cybersecurity Performance Goals.

Additional Assumptions:

- HCC members have mechanisms in place to maintain awareness of current threats and vulnerabilities, and the HCC has a mechanism to share and update situational awareness information.
- Core HCC activities such as information coordination and support will often provide critical assistance during a cyber or infrastructure failure event. This assessment does not assess usual coalition activities.
- Health care facilities, systems, and the HCC understand their integration into ESF-8 for information sharing, resource requests, and other emergency management support.
- Health care facilities, systems, and the HCC have mechanisms to develop internal and

external communications relevant to an incident and will work with a Joint Information System if one is activated within the jurisdiction.

- Health care facilities, systems, and the HCC have incident command processes that are understood and practiced.
- Health care facilities have facility-specific incident response plans in place including surge staffing plans; HCCs understand their supportive role as practical.

Related ASPR TRACIE Resources

- Cybersecurity Resources Page
- Cybersecurity Topic Collection
- Electronic Health Records and Downtime Procedures Topic Collection
- HCC Extended Downtime Health Care Delivery Impact Assessment
- HCC Resource Page
- 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
- HHS HPH Cybersecurity Performance Goals
- NIST Cybersecurity Framework (CSF) 2.0

Acknowledgements

Contributors and reviewers of this document are listed alphabetically and include: Representatives from **Arizona Coalition for Healthcare Emergency Response**; **Robert Bastani**, CISSP-ISSMP, CISM, CRISC, Senior Cyber Advisor, HHS ASPR; **Susan Sutton Clawson**, PhD, MPH, Field Officer- Region 3 and Interim Region 1, 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; **Charlee Hess**, MPA, Deputy Director, Cybersecurity Division, Critical Infrastructure Protection, HHS ASPR; **John Hick**, MD, ASPR TRACIE and Hennepin Healthcare; **Jodi Keller**, RN, Director of Health care System Emergency Preparedness and Response/ Central Region Health care Coordinator, COTS; **Angela Krutsinger**, FPO Supervisor (Acting), HHS ASPR; **Wai Ling Mui**, Lead Public Health Preparedness Analyst, ICF; Representatives from **Nebraska Medicine's Emergency Preparedness Program**; **Paul Pestel**, Arkansas Health Care Association; **Mary Russell**, EdD, MSN.

Health Care Coalition Cybersecurity Assessment

The following questions pertain to specific cybersecurity activities conducted by or internal to the HCC. Depending on the HCC, not all questions may apply.

HCC Cyber Activity	Yes/No/ Partial/NA	Additional Notes
1. Vulnerability Testing		
1.1. Has the HCC ever conducted an evaluation that lists systems used by the coalition for communications/monitoring, their "owners," and how to identify possible vulnerabilities?		
1.1.1. If so, has the HCC created a schematic map of the critical devices, platforms, software, servers, applications, and systems that the coalition uses to conduct its coordination activities?		
1.1.2. Does this mapping consider how integrated software could be used co-dependently and independently to restore some functionality?		
1.1.3. Have IT systems been prioritized for restoration based on functionality and continuity of critical operations?		
1.2. Do the HCC's software / hardware platform service providers and operators conduct vulnerability testing (penetration testing/attack simulations) of public-facing or permission-based systems the coalition uses for data / incident management?		
1.2.1. If so, are they required to provide attestation of their work to the HCC?		
1.3. Has the HCC taken measures to ensure servers and other hardware are protected from utilities failure, flooding, and other risks?		
1.4. Does the HCC have "clean" computers that are isolated from networks and software upgrades that can be relied upon in case of a cyber incident?		

HCC Cyber Activity	Yes/No/ Partial/NA	Additional Notes
2. Cyber Hygiene		
2.1. Do you know what external programs and software could become a vector into HCC and other systems (e.g., Google docs, Dropbox, chat programs, sending files)?		
2.2. Does the HCC utilize platforms and programs that balance ease of sharing across systems with minimizing cybersecurity and operational vulnerabilities?		
2.3. Does the HCC support email security practices within the coalition?		
2.4. Does the HCC support multifactor authentication for existing software and tools?		
2.5. Does the HCC utilize encryption techniques to protect information?		
3. Access Management		
3.1. Does the HCC implement unique credentialing among coalition members for systems, software, and/or tools?		
3.2. Does the HCC have a credential review and revoking protocol in place to ensure personnel no longer in need of access are removed from systems, software, and tool access?		
3.3. Does the HCC maintain separate user and admin accounts?		

HCC Cyber Activity	Yes/No/ Partial/NA	Additional Notes
4. Facility Security		
4.1. Does the HCC have mechanisms to address access management needs for coalition personnel (e.g., badging, screening) that includes education-based protections (e.g., preventing piggybacking)?		
4.2. Does the HCC or its host have a mechanism to address the physical security of the servers, system hardware, and T1 or other trunk lines used by the HCC?		
4.3. Does the HCC have access to generators/uninterruptable power supplies?		
5. Personnel		
5.1. Does the HCC have a cybersecurity/IT expert to assist with risk analysis?		
5.1.1. If not, does the HCC have support from a health care system or other entity in conducting a risk analysis and providing recommendations?		
5.2. Are the HCC personnel educated on basic cyber hygiene practices?		
5.3. Are the HCC personnel trained to recognize and report potential issues related to cyber incidents? Do they know what to look for?		
5.4. If the HCC does not have dedicated IT staff, do you know who to contact if a system is exhibiting unusual behavior?		
5.5. Are the HCC personnel trained in using backup systems?		
6. Training and Exercises		
6.1. Has the HCC conducted any cybersecurity training or exercises? Who provides it? • Internal training for HCC staff • External training for members and/or partners		

HCC Cyber Activity	Yes/No/ Partial/NA	Additional Notes
• Training focused on best practices for cyber hygiene • Training and exercises focused on cyber incident response		
6.2. Does the HCC regularly meet/engage as a group to discuss cyber initiatives?		
6.2.1. If so, have you brought in external experts to discuss best practices and vulnerabilities?		
7. Threat Monitoring		
7.1. Does the HCC have a process to maintain situational awareness of cyber incidents occurring within the jurisdiction or that pose national-level risk?		
7.2. Does the HCC have a process to engage with cyber/IT experts on new threats/vulnerabilities?		
7.3. Does the HCC have a process to identify a cyber-attack or systems failure and shut down affected systems?		
7.4. Is there a protocol for who decides when an “incident” has occurred and is there an established threshold?		
8. Incident Response & Management		
8.1. Does the HCC have a cyber/IT systems incident response plan?		
8.1.1. Have you defined roles and responsibilities?		
8.2. Is there a process for supporting a coalition member affected by a systems failure/cyber incident when the HCC is not affected?		

	8.2.1. Do coalition members understand what support can be provided by the coalition during a cyber event?		
	8.2.2. Is there a plan for the HCC to support affected facilities?		
	8.2.3. Have hospitals/health care systems discussed the implications of a cyber event on members and what response strategies may be advisable (e.g., plans for limited EMS diversion, deferring certain procedures)? This may include certain agreements on the limits of assistance provided or conditions (e.g., no EMS diversion unless all elective procedures stopped, or an agreement to provide IT or personnel support to encourage service continuity).		
8.3.	Does the HCC have a cybersecurity/IT expert that can advise the coalition in the event of a cyber incident (cyber response)?		
	8.3.1. If not, does the HCC have a plan for obtaining response support?		
9. Communication and Coordination			
9.1.	Does the HCC have a cyber incident communication plan to include incident messaging (who, how, how often, message approval)?		
	9.1.1. If not, is the HCC planning to develop one?		
	9.1.2. How will the HCC maintain situational awareness, engagement, and communications after an incident?		
9.2.	Does the HCC have dedicated or designated mechanisms for communicating (e.g., radios, phones, CAD)?		
	9.2.1. Are there backup mechanisms (e.g., satellite internet, and/or requesting deployable resources from cellular carriers disaster assistance teams) if planned devices are unavailable (e.g., downed phone lines, internet calling outage, portable cellular connectivity)?		

HCC Cyber Activity	Yes/No/ Partial/NA	Additional Notes
9.3. Are there established emergency POCs at the coalition level and member level?		
9.3.1. Is there an understanding of who to contact and how (if usual communications are down) in case of a cyber incident to include: • Third-party vendor coordination (who to contact) • Emergency external points of contact (e.g., EMS) • Agency/Law Enforcement • State and Local Agencies (e.g., emergency management, public health)		
10. Legal Considerations		
10.1. If a ransom is demanded during a cyber-attack, is there a plan for who has the authority to respond on behalf of the HCC?		
10.1.1. Does the HCC know the authorities that would need to be contacted in the event of an attack (e.g., Federal Bureau of Investigation [FBI], CISA, local law enforcement)?		
10.1.2. Has the HCC engaged in pre-event discussions to identify who is authorized to legally represent the coalition (e.g., host entity counsel, jurisdictional representative, or pro bono legal support)?		