Central Florida

Disaster Medical Coalition

Preparing Central Florida's Best for the Worst, Together!

Cybersecurity Assessment Summary Report

Approved by CFDMC Board June 4, 2025

FY24-25 Cybersecurity Assessment Summary Report

This report summarizes responses from the FY24-25 Cybersecurity Survey. It includes organizational participation by type, highlights of the findings, recommended actions, and resources to strengthen healthcare cybersecurity readiness.

Table of Contents

Executive Summary

The Florida Health Care Coalitions collaborated to develop and deploy a Cybersecurity Assessment Survey aimed at evaluating the cyber readiness of healthcare organizations across the region. The survey questions were based on the ten essential Cybersecurity Performance Goals (CPGs) outlined by the U.S. Department of Health and Human Services (HHS) for the Healthcare and Public Health (HPH) Sector. The survey was distributed to Coalition member organizations on March 21, 2025, and remained open through March 31, 2025.

This report summarizes the findings from the FY24–25 Cybersecurity Survey, at both the statewide and regional (Coalition) levels, including organizational participation by type, highlights of key cybersecurity practices, and visualizations of responses categorized by organization type. Statewide results demonstrated strong adoption of foundational security practices, with 96.2% of respondents reporting measures to mitigate known vulnerabilities, 96.2% deploying email security protections, and 88.7% enforcing credential revocation protocols. However, gaps remain in areas such as multifactor authentication adoption (82.7%) and comprehensive workforce cybersecurity training (83.8%), particularly among smaller or resource-limited organizations.

The survey findings emphasize the critical need to address cybersecurity vulnerabilities, which pose a heightened risk to Communities Most Impacted by Disasters, including underserved populations and rural healthcare providers. To support risk reduction, the report provides recommended action steps, promotes the adoption of best practices such as the Health Industry Cybersecurity Practices (HICP) and the National Institute of Science and Technology (NIST) Cybersecurity Framework (CSF), and offers curated resources for training and technical assistance. Overall, the results closely align with the priorities outlined in the HHS ASPR 2024–2029 Strategic Plan to advance cybersecurity resilience across the healthcare sector.

Cybersecurity Impact on Communities Most Impacted by Disasters (CMID)

A cybersecurity incident in the healthcare sector can have disproportionately severe consequences for Communities Most Impacted by Disasters (CMID), including underserved populations, rural communities, older adults, and those with limited access to healthcare. The statewide assessment data reveals that while many healthcare organizations have foundational cybersecurity measures in place—such as multifactor authentication (82.7%) and cybersecurity training (83.8%)—these protections are not yet universally adopted across all organization types, including long-term care, behavioral health, and ambulatory services, which often serve vulnerable populations. In the event of a cyberattack that disrupts healthcare operations, these communities are at greater risk of care delays, communication breakdowns, and medical errors due to limited redundancy in care options and infrastructure. Strengthening cyber resilience in all healthcare settings, especially those categorized as “Other” in the assessment (e.g., dialysis centers, home health, assisted living), is essential to minimizing harm and ensuring equity in emergency response and continuity of care.

Response Summary by Organization Type

Responses were received from a variety of organization types. The most common types include:

Statewide (266 Responses):
* Other – 113 responses
(Behavioral Health, Ambulatory Surgery Centers, Dialysis Clinics, Assisted Living Facilities, Public Health Units) (See Appendix A for full breakdown by facility type)
* Hospital – 50 responses
* Long Term Care – 45 responses
* Department of Health – 33 responses
* Emergency Management – 17 responses

CFDMC (55 Responses):
* Other – 29 responses
(Behavioral Health, Ambulatory Surgery Centers, Dialysis Clinics, Assisted Living Facilities, Public Health Units) (See Appendix A for full breakdown by facility type)
* Hospital – 8 responses
* Long Term Care – 6 responses
* Department of Health – 2 responses
* Emergency Management – 5 responses
* Emergency Medical Services – 5 responses

Survey Questions and Responses (Statewide & CFDMC)

Below are the number/percentage of responses for each question, both statewide and for CFDMC (Region 5):

1) The organization mitigates against known vulnerabilities; it has measures in place and works to reduce the likelihood of threat actors exploiting known vulnerabilities to breach organizational networks that are directly accessible from the Internet.

Statewide	CFDMC
266 Responses	55 Responses
No – 2 (1%)	No – 0 (0%)
Not Sure – 8 (3%)	Not Sure – 2 (4%)
Yes – 256 (96%)	Yes – 53 (96%)

2) The organization has email security; it has measures in place and works to reduce risk from common email-based threats such as email spoofing, phishing, and fraud.

Statewide	CFDMC
266 Responses	55 Responses
No – 3 (1%)	No – 1 (1%)
Not Sure – 7 (3%)	Not Sure – 2 (3%)
Yes – 256 (96%)	Yes – 52 (96%)

3) The organization has multifactor authentication; it utilizes this feature to add a critical, additional layer of security where safe and capable to protect assets and accounts directly accessible from the Internet.

Statewide	CFDMC
266 Responses	55 Responses
No – 23 (9%)	No – 4 (7.5%)
Not Sure – 22 (8%)	Not Sure – 9 (16.5%)
Yes – 221 (83%)	Yes – 42 (76%)

4) The organization has its staff undergo basic cybersecurity training to ensure organizational users learn and perform more secure behaviors.

Statewide	CFDMC
266 Responses	55 Responses
No – 19 (7%)	No – 3 (5%)
Not Sure – 23 (9%)	Not Sure – 10 (18%)
Yes – 223 (84%)	Yes – 42 (77%)

5) The organization deploys encryption to maintain confidentiality of sensitive data and integrity of Information Technology (IT) and Operational Technology (OT).

Statewide	CFDMC
266 Responses	55 Responses
No – 10 (4%)	No – 1 (2%)
Not Sure – 30 (11%)	Not Sure – 10 (18%)
Yes – 226 (85%)	Yes – 44 (80%)

6) The organization promptly revokes credentials for departing workforce members, including employees, contractors, affiliates, and volunteers to prevent unauthorized access to organization accounts or resources.

Statewide	CFDMC
266 Responses	55 Responses
No – 2 (1%)	No – 1 (2%)
Not Sure – 27 (10%)	Not Sure – 10 (18%)
Yes – 237 (89%)	Yes – 44 (80%)

7) The organization trains in basic incident preparedness to ensure safe and effective organizational responses to, restoration of, and recovery from significant cybersecurity incidents.

Statewide	CFDMC
266 Responses	55 Responses
No – 16 (6%)	No – 2 (4%)
Not Sure – 32 (12%)	Not Sure – 8 (14%)
Yes – 218 (82%)	Yes – 45 (82%)

8) The organization uses unique credentials inside organizations' networks to detect anomalous activity and prevent attackers from moving laterally across the organization, particularly between IT and OT networks.

Statewide	CFDMC
266 Responses	55 Responses
No – 6 (2%)	No – 2 (3.5%)
Not Sure – 67 (25%)	Not Sure – 13 (23.5%)
Yes – 193 (73%)	Yes – 40 (73%)

9) The organization has separate user and privileged accounts; it establishes secondary accounts to prevent threat actors from accessing privileged or administrative accounts when common user accounts are compromised.

Statewide	CFDMC
266 Responses	55 Responses
No – 6 (2%)	No – 1 (2%)
Not Sure – 71 (27%)	Not Sure – 15 (27%)
Yes –189 (71%)	Yes – 39 (71%)

10) The organization has vendor/supplier cybersecurity requirements; it identifies, assesses, and mitigates risks associated with third party products and services.

Statewide	CFDMC
266 Responses	55 Responses
No – 12 (5%)	No – 2 (4%)
Not Sure – 49 (18%)	Not Sure – 11 (20%)
Yes – 205 (77%)	Yes – 42 (76%)

Optional questions provided the following information:

- CFDMC respondents stated that in a cyber security breach, they would internally notify leadership and IT, and externally notify the FBI, CISA, AHCA, their IT vendor and/or liability carrier, and CFIX.
- CFDMC respondents stated that they have multiple redundant communication methods, including cell phones, analog and VoIP phones, text, email, Teams, and other platforms such as Everbridge and EMResource.
- CFDMC respondents stated that after the initial notifications, additional actions they would take include shutting down IT systems, isolating potential breached accounts, devices and applications, and going to back-up servers.

Gaps & Mitigation Strategies Identified Through the Cybersecurity Assessment

The FY24–25 Cybersecurity Assessment not only evaluated current capabilities but also identified gaps and supported the identification of mitigation strategies to reduce risk across diverse healthcare settings. Based on the findings, several statewide and regional gaps and key strategies emerged:

- Adoption of Multifactor Authentication (MFA): Increasing the implementation of MFA remains a critical step to prevent unauthorized access to sensitive systems. Survey results showed 82.7% adoption, indicating room for further outreach and support.
- Enhanced Workforce Training: With 83.8% of organizations conducting basic cybersecurity training, expanding this practice to reach 100% participation will strengthen security culture and user awareness across the sector.
- Network Segmentation and Unique Credentials: Organizations that use unique credentials within networks (as reported by over 80%) are better positioned to detect and respond to anomalous activity. Promoting this strategy more broadly, especially in smaller or resource-limited facilities, is recommended.
- Third-Party Risk Management: The assessment highlighted the importance of requiring cybersecurity standards from vendors and suppliers. Incorporating contractual expectations and routine assessments of third-party partners is a key mitigation approach.
- Credential Revocation Protocols: Promptly revoking credentials for departing staff is a simple but critical strategy that 88.7% of respondents have already implemented. Ensuring this practice is formalized and automated can further reduce insider threat risks.

These strategies reflect foundational elements recommended in the HHS ASPR 2024–2029 Strategic Plan and serve as practical, scalable interventions that healthcare organizations—especially those serving vulnerable populations—can adopt to reduce exposure to cyber threats.

In addition, CFDMC will participate in a regional initiative funded through UASI to develop a regional cyber response plan.

Recommended Action Items to Strengthen Healthcare Cybersecurity Statewide

- Conduct regular cybersecurity risk assessments and gap analyses.
- Participate in statewide, regional or coalition-led cyber exercises.
- Establish formal cybersecurity incident reporting protocols.
- Incorporate cyberattack scenarios into downtime and business continuity planning.
- Implement third-party vendor cybersecurity reviews and security requirements.
- Launch ongoing cybersecurity awareness and workforce training campaigns.
- Share real-world case studies of healthcare cyber incidents to reinforce preparedness.
- Engage with regional cybersecurity collaboratives and healthcare-specific information sharing groups.
- Pursue cybersecurity grant funding and technical assistance opportunities (e.g., ASPR HPP, CISA programs).

Conclusion & Alignment with HHS ASPR 2024–2029 Cybersecurity Priorities

The FY24–25 Cybersecurity Assessment provides critical insight into the current cybersecurity posture of healthcare organizations across the region. Findings from this assessment indicate promising adoption of core cybersecurity practices while also highlighting opportunities for improvement that align with the HHS ASPR 2024–2029 National Objectives for Funding Opportunity (NOFO) priorities.

According to the statewide survey data:
- 96.2% of respondents reported having measures in place to mitigate known vulnerabilities. (CFDMC reported 96%)
- 96.2% have email security protections to combat spoofing, phishing, and fraud. (CFDMC reported 96%)
- 82.7% reported utilizing multifactor authentication to protect internet-accessible assets. (CFDMC reported 76%)
- 83.8% have conducted basic cybersecurity training for staff. (CFDMC reported 77%)
- 85.0% reported deploying encryption to safeguard sensitive data. (CFDMC reported 80%)
- 88.7% promptly revoke credentials for departing personnel to prevent unauthorized access. (CFDMC reported 80%)

These findings align with ASPR's strategic focus on improving organizational readiness, incident response capabilities, and information system resilience across the healthcare sector. The inclusion of training, multifactor authentication, encryption, and identity/access control supports the foundational goals outlined in the 2024–2029 Strategic Plan to improve sector-wide preparedness for cyber threats.

Importantly, the "Other" organization type category—comprising behavioral health providers, ambulatory surgery centers, dialysis clinics, and other health agencies—demonstrates that cybersecurity efforts must extend beyond traditional acute care settings to the full spectrum of healthcare partners involved in emergency preparedness and response.

As the Florida Health Care Coalitions in partnership with Cyber Florida, CISA, FDOH, and ASPR continues to advance the cybersecurity resilience of the healthcare system, this assessment serves as a tool to help organizations benchmark their current practices, identify priority actions, and demonstrate alignment with national strategic goals.

Resources for Healthcare Cybersecurity Best Practices and Training

- HHS ASPR TRACIE Cybersecurity Resources: https://asprtracie.hhs.gov/cybersecurity
- HHS 405(d) Health Industry Cybersecurity Practices (HICP): https://405d.hhs.gov/
- CISA Healthcare and Public Health Sector Resources: https://www.cisa.gov/healthcare-and-public-health-hph-sector
- NIST Cybersecurity Framework (CSF): https://www.nist.gov/cyberframework
- Health Sector Cybersecurity Coordination Center (HC3): https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html
- MS-ISAC Free Cybersecurity Services for Critical Infrastructure: https://www.cisecurity.org/ms-isac
- CISA Cyber Essentials Training: https://www.cisa.gov/cyber-essentials
- Health Information Sharing and Analysis Center (H-ISAC): https://h-isac.org/
- National Cybersecurity Alliance Resources: https://staysafeonline.org/