HEALTHCARE & PUBLIC HEALTH SECTOR CYBERSECURITY

Sector Overview

This resource is for stakeholders in Florida's Healthcare and Public Health sector. It includes hospitals, clinics, imaging providers, public health agencies, and healthcare-related organizations. The sector delivers essential medical services statewide. Ransomware disruptions can halt treatments, delay diagnostics, and put patient safety at risk.

Top Vulnerabilities

- **Unsupported Clinical & Imaging Equipment**
  - Many facilities use MRI, CT, and other diagnostic machines with outdated operating systems that cannot be patched.
- **Unpatched EHR and Lab Systems**
  - Legacy electronic health records and lab management platforms often run on obsolete software, making them easy ransomware targets.
- **Infrequent Ransomware-Specific Drills**
  - Less than half of providers conduct exercises that simulate impacts to clinical care and medical devices.
- **Third-Party Vendor Risks in Care Delivery**
  - Reliance on external diagnostic, claims, and records vendors creates exposure if those partners lack MFA or incident monitoring.

Ransomware Threat Profile

About 28% of Florida healthcare providers meet DHS ransomware readiness standards. This ranks above some sectors but still leaves major gaps. Healthcare remains a top ransomware target due to valuable patient data, strict compliance requirements, and the use of interconnected medical systems.

Year	Total Breaches	Ransomware Breaches	Records Affected by Ransomware	% of Total Records
2016	328	30 (9%)	324	2%
2017	358	58 (16%)	1,887	36%
2018	369	37 (10%)	2,800	18%
2019	511	72 (14%)	4,739	11%
2020	663	203 (31%)	18,176	51%
2021	715	222 (31%)	26,754	44%
2022	720	204 (28%)	29,246	51%
2023	745	165 (22%)	84,491	51%
2024*	566	61 (11%)	116,946	69%

Note: From 2016 to 2021, ransomware attacks grew from 9% to over 30% of all healthcare data breaches. The percentage of ransomware-related breaches declined slightly after 2021, but the share of affected patient records remained high and peaked at 69% in 2024.
*2024 data is incomplete and only includes incidents reported through October 31, per OCR/HHS.

Notable Incidents

- **Tallahassee Memorial Healthcare (2025):** TMH announced a data breach linked to a third-party vendor's legacy data migration error, which exposed patient information and forced internal systems offline. While not confirmed as ransomware, this incident reflected key vulnerabilities typically exploited in such attacks.
- **Akumin Diagnostics, Broward County (2023):** Ransomware disabled imaging systems for several weeks, impacting patient diagnostics and treatments, with potential exposure of personal and protected health information (PHI).
- **UF Health Central Florida (2021):** Ransomware forced emergency patient diversions and disrupted access to electronic health records for weeks. Staff reverted to manual documentation, which slowed care delivery and created operational strain across multiple facilities.

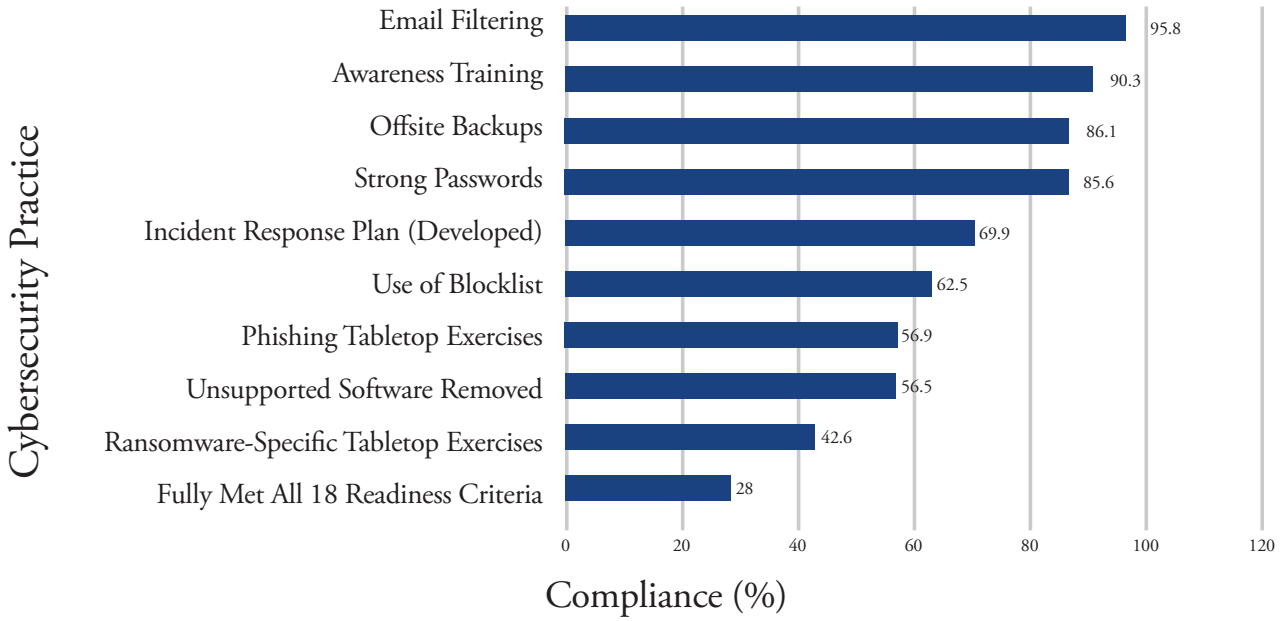
FIU Jack D. Gordon Institute for Public Policy
JGI@fiu.edu
CYBER FLORIDA AT THE UNIVERSITY OF SOUTH FLORIDA

HEALTHCARE & PUBLIC HEALTH SECTOR CYBERSECURITY

Action Checklist

- Develop and test ransomware Incident Response Plans for EHR systems, medical devices, and life support equipment.
- Enforce MFA across clinical, administrative, and vendor-connected systems.
- Conduct annual tabletop drills simulating ransomware disruption to emergency care and diagnostics.
- Replace or segment unsupported medical devices and imaging systems from main networks.
- Maintain HIPAA-compliant, offline backups of patient records, imaging data, and scheduling systems.
- Assign a cybersecurity lead (CISO or equivalent) with healthcare IT and clinical systems expertise.

Ransomware Readiness Gaps - Government Facilities (2024



Note: In 2024, only 28% of Florida healthcare providers met all DHS ransomware readiness standards. While this is above several other sectors, persistent vulnerabilities in outdated medical equipment and insufficient testing leave patient care at risk.

State-Funded Resources & Education

Technical Tools

- **CISA Ransomware Readiness Assessment (CSET)**
- **Health Sector Cybersecurity Coordination Center (HC3)**

Templates & Planning

- **Cyber Florida Incident Response Plan Templates**
  Available Upon Request
- **NIST Cybersecurity Framework**
  (https://www.nist.gov/cyberframework)
- **HICP - Health Industry Cybersecurity (401(d))**

State-Funded Resources

- **FIU Cyber Leadership Courses**
  (https://gordoninstitute.fiu.edu/cybersecurity-policy/training/cybersecureflorida/index.html)
- **CISA Cyber Hygiene Services**
  Free Assessments & Scans
  (https://www.cisa.gov/resourcestools/ programs/cyberhygiene-services)

FIU Jack D. Gordon Institute for Public Policy
JGI@fiu.edu
CYBER FLORIDA AT THE UNIVERSITY OF SOUTH FLORIDA