MIDWEST QIN-QIO

Midwest QIN-QIO's Cybersecurity Mission

Purpose and CMS Alignment

- The 13th SoW cybersecurity offering supports CMS's goals for patient safety, continuity of care, and health system resilience
- Cybersecurity is positioned as a quality and safety issue, not solely an IT function—cyber incidents directly impact care delivery, privacy, and trust
- Services are non-punitive, confidential, and improvement-focused, consistent with the QIN-QIO mission

Who the Offering Is For

- Designed for small-to-medium healthcare providers, including:
- Hospitals and Critical Access Hospitals
- Skilled Nursing Facilities and long-term care
- Rural and underserved providers
- Ambulatory, home health, and community-based organizations
- Especially beneficial for organizations with limited cybersecurity staff or resources

What QIN-QIOs Provide (At No Cost)

- Cybersecurity readiness and maturity assessments tailored to healthcare operations
- Gap identification aligned to recognized frameworks (e.g., NIST CSF, HICP)
- Actionable remediation roadmaps prioritized by risk and feasibility
- Education and awareness for leadership and frontline staff
- Incident preparedness guidance, including tabletop exercises and response planning

Provider-Focused Value

- Helps providers:
  - Reduce exposure to ransomware and data breaches
  - Strengthen protection of ePHI and clinical systems
  - Improve downtime preparedness and recovery
  - Meet payer, regulatory, and accreditation expectations
- Focuses on practical controls, not theoretical compliance

MIDWEST QIN-QIO

Integration With Quality Improvement

- Cybersecurity is embedded into broader quality and patient safety initiatives
- QIN-QIOs help align cybersecurity improvements with:
- Risk management programs
- Emergency preparedness requirements
- Governance and leadership accountability

Workforce and Culture of Security

- Addresses the human factor through:
  - Phishing and social engineering awareness
  - Role-based cybersecurity education
  - Leadership engagement and governance practices
- Supports development of a culture of shared responsibility for cyber safety

Incident Response and Resilience

- Assistance with:
  - Developing or refining incident response plans
  - Preparing for ransomware and operational disruptions
  - Improving coordination between clinical, IT, and executive teams
- Focus on maintaining patient care during cyber events.

Confidentiality and Trust

- Participation data and findings are not shared with CMS for enforcement purposes
- The QIN-QIO acts as a trusted, neutral partner, not a regulator
- Providers control how findings are used internally

Expected Outcomes

- Improved cybersecurity posture and risk awareness
- Reduced likelihood and impact of cyber incidents
- Stronger organizational resilience and preparedness
- Better protection of patients, staff, and communities

Call to Action for Providers

- Engage early to maximize benefit during the 13th SoW period
- Identify executive, clinical, and IT champions for participation
- Treat cybersecurity as a core patient safety and quality priority

This material was prepared by Midwest QIN-QIO, a Quality Innovation Network-Quality Improvement Organization, under contract with the Centers for Medicare & Medicaid Services (CMS), an agency of the U.S. Department of Health and Human Services (HHS). Views expressed in this material do not necessarily reflect the official views or policy of CMS or HHS, and any reference to a specific product or entity herein does not constitute endorsement of that product or entity by CMS or HHS. This material is for informational purposes only and does not constitute medical advice; it is not intended to be a substitute for professional medical advice, diagnosis or treatment. 13thSOW-QIN-QIN-01/29/26-133