Quality Improvement Organizations
Sharing Knowledge. Improving Health Care.
CENTERS FOR MEDICARE & MEDICAID SERVICES

SUPERIOR HEALTH Quality Alliance
Great Lakes Region

Protect Your Patients. Protect Your Organization.

Practical cybersecurity actions for nursing homes, clinics, and hospitals.

Cyber threats can disrupt patient care, expose sensitive information, and interrupt essential operations. Cybersecurity is not only an information technology (IT) responsibility. It requires informed employees, strong technical safeguards, and practiced response procedures throughout the organization.

Cybersecurity Awareness Month | October 2026

Security Awareness Training: Your First Line of Defense

Technology alone cannot stop every cyber threat. Employees are frequently targeted through phishing and social engineering. Regular, practical training helps staff recognize suspicious activity, handle patient and organizational information safely, and know how to report concerns quickly.

Key message:
An informed workforce can turn a potential incident into a timely report instead of a damaging compromise.

Build a Security-Aware Workforce

Train Everyone

Provide security awareness training during onboarding and refresher education at least annually. Include employees, contractors, temporary staff, and volunteers who access organizational systems or information.

Reinforce Throughout the Year

Share short reminders when threats change, after policy updates, and during Cybersecurity Awareness Month. Use phishing simulations as a learning opportunity, not a punishment.

Make Training Relevant

Use realistic health care examples, including phishing, credential theft, inappropriate disclosure of patient information, ransomware warning signs, and safe use of mobile devices.

Make Reporting Easy

Tell staff exactly how to report suspicious messages, lost devices, unusual system activity, or accidental disclosures. Prompt reporting helps the organization respond sooner.

Cover Down on the Basics

Cybercriminals look for easy targets. The Cybersecurity & Infrastructure Security Agency (CISA) encourages organizations to begin with four essential steps that help safeguard data and equip employees to stop attacks before they happen.

1 Teach Employees to Avoid Phishing Scams

Train staff to recognize and report suspicious emails, texts, links, attachments, urgent payment requests, and requests for sensitive information.

- Conduct awareness training and phishing exercises.
- Provide a clear reporting method.
- Reinforce: pause, verify, and report.

2 Require Strong Passwords

Require long, unique passwords for organizational accounts and prevent password reuse or sharing. An approved password manager can help users maintain unique credentials.

- Review password requirements.
- Prohibit shared credentials.
- Protect privileged and service accounts.

3 Require Multifactor Authentication

Multifactor Authentication (MFA) adds another layer of protection beyond a password. Require MFA for email, remote access, cloud services, and administrative accounts. Use phishing-resistant MFA where available.

- Prioritize high-risk and privileged accounts.
- Enroll all eligible users.
- Review and remove inactive accounts.

4 Update Business Software

Outdated software may contain known vulnerabilities. Install security updates promptly and replace unsupported software and devices.

- Maintain an inventory of systems and devices.
- Establish patching responsibilities and timelines.
- Verify updates were successfully applied.

Strengthen Cyber Resilience

CISA also identifies additional organizational steps that help reduce risk and improve recovery. Use this checklist to identify priorities for your organization.

- ☐ **Use Logging and Monitoring**
  Enable logging on critical systems, review logs for unusual activity, and establish alerts for suspicious behavior.
- ☐ **Back Up Critical Data**
  Maintain secure backups, separate them from production systems, and test restoration procedures.
- ☐ **Encrypt Sensitive Information**
  Protect sensitive data in transit and at rest, including information stored on laptops, mobile devices, and portable media.
- ☐ **Have an Incident Response Plan and Use It**
  Document response procedures, define roles and contacts, and practice the plan through tabletop exercises.
- ☐ **Prepare for System Disruptions**
  Maintain downtime and business continuity procedures so staff can continue essential care and operations during technology outages.

Cybersecurity Awareness Month Action Challenge

Choose at least one improvement to complete this month:

- ☐ Complete or refresh security awareness training.
- ☐ Run a phishing simulation and review lessons learned.
- ☐ Enable MFA for eligible accounts.
- ☐ Verify critical systems are patched.
- ☐ Test backup restoration procedures.
- ☐ Review or exercise the incident response plan.
- ☐ Confirm downtime procedures are current.

Superior Health Quality Alliance is Here to Help

Superior Health Quality Alliance can provide participating nursing homes, clinics, and hospitals with cybersecurity education, technical assistance, and resources to support awareness, preparedness, and resilience.

Contact: info@superiorhealthqa.org

Website: superiorhealthqa.org

Source and additional resources: CISA Cybersecurity Awareness Month Toolkit
Adapted from guidance published by the U.S. Cybersecurity and Infrastructure Security Agency (CISA). Organizations should align actions with their own policies, risk assessments, contractual requirements, and applicable laws and regulations.

Quality Improvement Organizations
Sharing Knowledge. Improving Health Care.
CENTERS FOR MEDICARE & MEDICAID SERVICES

SUPERIOR HEALTH Quality Alliance
Great Lakes Region

This material was prepared by the Superior Health Quality Alliance, 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. 13SOW-QINQIO-R4-26-173 091426