COVID-19

READY, SET, GO!

CHECKLIST - CYBERSECURITY PLANNING

GET READY

Create or Review Your Cybersecurity Event Action Plan Today!

We made it easy to review or enhance your facility's cybersecurity plan.

View Alliant's Emergency Preparedness Planning (EPP): A Guide to Resources and Templates for Nursing Homes additional resources, **NOW!**

Create a simple grab-and-go guide or poster that highlights essential information and immediate actions to take:

- □ Notify the administrator or manager on duty immediately.
- □ Instruct staff to log off computers and implement downtime procedures.
- □ Execute policy for caring for patients on medical devices connected to facility systems.
- □ Advise/assist patients, residents and visitors to disconnect from the facility's wireless internet.

Ensure key elements are addressed, including a phone tree identifying internal and external contacts for immediate notification.

- ✓ Internal Notifications:
  - Information Technology (IT)
  - Risk Management
  - Legal Counsel
  - Human Resources
- ✓ External Notifications:
  - Vendors
  - Local law enforcement
  - Cybersecurity and Infrastructure Security Agency
  - Department of Health and Human Services
  - Federal Bureau of Investigation (FBI)
- ✓ Essential information to share with an incident response team, such as:
  - One site versus multiple sites.
  - Isolated outage versus full network outage.
  - Status of phone tree contacts.
  - Key stakeholder communication plan.

Important Tips

Assume a cybersecurity event is a malicious incident until proven otherwise.

Review policies and plans annually and after an incident.

Monitor local, state and federal requirements for updating all emergency preparedness plans.

Consider all systems that the incident might impact:

- □ Staffing
- □ Central and remote patient monitoring
- □ Emergency and safety systems
- □ Nurse call systems
- □ Imaging
- □ Pharmacy
- □ Environmental controls
- □ Other network-reliant systems
- □ Lab devices, text paging

Conduct after-action reviews and incorporate key takeaways and lessons learned into plans.

GET SET

Do this to make sure you are ready.

- □ Exercise your plans and policies regularly.
- □ Ensure staff onboarding materials include proper downtime and safe internet use procedures for your facility.
- □ Instruct staff to report any suspicious emails or internet activity immediately.
- □ Provide staff with clear and approved talking points for discussing cybersecurity with patients and residents.

GO!

Do this when you activate your plan.

- □ Maintain open communication with staff, residents and visitors throughout the incident.
- □ Adjust downtime processes and plans as information becomes known.
- □ Collaborate with IT, risk management and legal teams.
- □ Activate your call tree and other notification systems.
- □ Provide information on available mental health support resources to building occupants after actual or averted incidents.

This material was prepared by Alliant Health Solutions, a Quality Innovation Network – Quality Improvement Organization (QIN – QIO) 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. Publication No.12SOW-AHS-QIN-QIO-TO1-NH-TO1-PCH-5828-06/04/24

ALLIANT HEALTH SOLUTIONS IPRO QIN-QIO HQIC ESRD QIN–QIO Quality Innovation Network - Quality Improvement Organizations CENTERS FOR MEDICARE & MEDICAID SERVICES iQUALITY IMPROVEMENT & INNOVATION GROUP

www.alliantquality.org