

Introduction to Initiative 4: Cybersecurity Resilience for Rural NY

New York's Rural Health Transformation plan to strengthen
cybersecurity for our rural healthcare facilities



Presented by the Department of Health
August 17 | 3:00 – 3:30 p.m. ET



This project is supported by the Centers for Medicare & Medicaid Services (CMS) of the U.S. Department of Health and Human Services (HHS) as part of a financial assistance award totaling \$212,058,207.80 in Budget Period 1 with 100 percent funded by CMS/HHS. The contents are those of the author(s) and do not necessarily represent the official views of, nor an endorsement, by CMS/HHS, or the U.S. Government.

Rural Health Transformation Program (RHTP) Initiatives Overview

New York's Rural Health Transformation Program includes four major initiatives designed to strengthen rural health care access, sustainability, workforce, technology, and resilience

Initiative 1

Rural Community
Health Integration

Initiative 2

Strengthening
Rural
Communities with
Technology-
Enhanced Primary
Care (Patient-
Centered Medical
Home)

Initiative 3

Rural Roots:
Building a
Sustainable
Rural Healthcare
Workforce

Initiative 4

Investments in
Technology
Innovation &
Cybersecurity
Resilience

Why We're Here

Today's session will provide a brief overview of the initiative, why it matters, and what participation involves.

1

How Initiative 4 fits within New York's broader Rural Health Transformation Program

2

Why cybersecurity resilience matters for operations and care continuity

3

What to expect from the guided cybersecurity resilience assessment

4

How the web-based assessment platform supports the process

5

How your facility can express interest and take the next steps

For further information contact: rhtpcyber@health.ny.gov

The First Phase of a Broader Effort

The current phase is focused on rural hospitals and the cybersecurity resiliency assessment.

Year 1

Participating rural hospitals complete the assessment to help identify current needs, common priorities, and future planning opportunities. Facilitate cyber risk mitigation efforts for rural hospitals by setting up shared security services where relevant and/or provide funding support for specific risk mitigation projects.

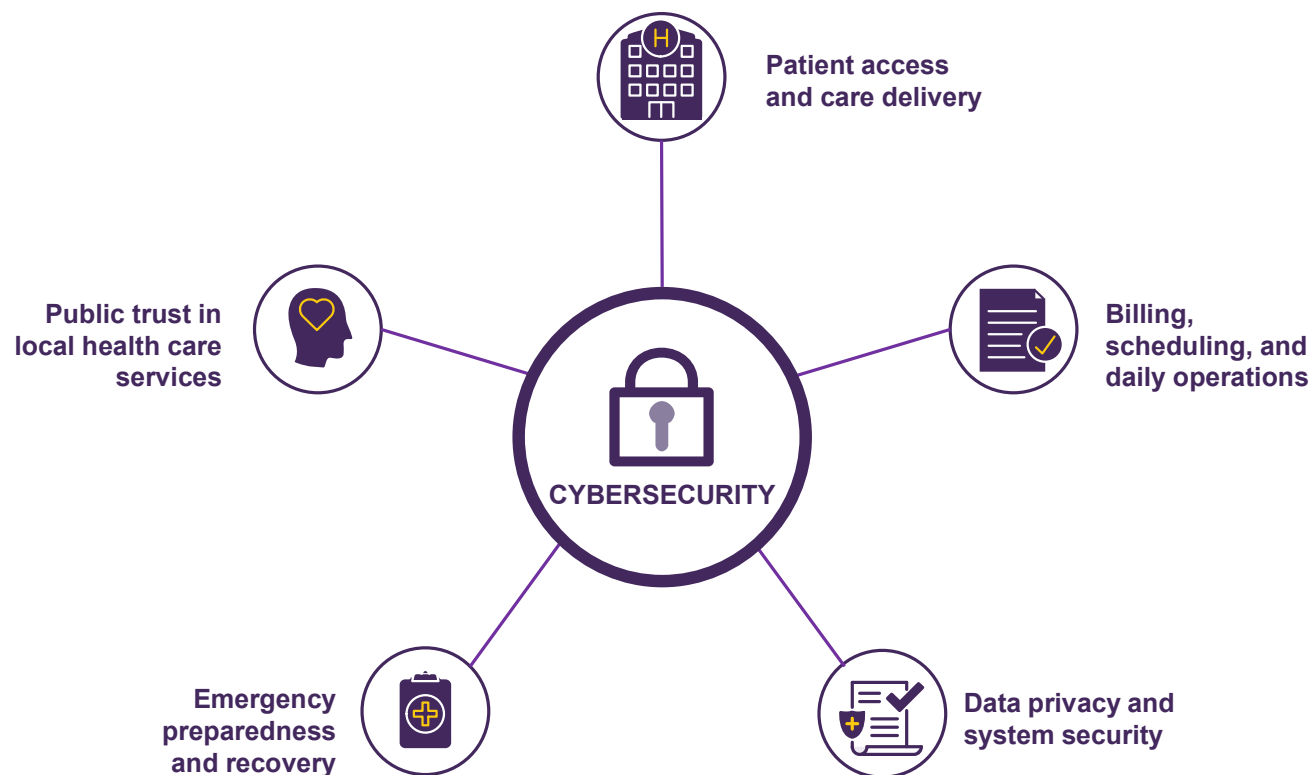
Future (years 2-5)

The broader cybersecurity resilience effort will expand to additional rural health care entities, such as pharmacies, nursing homes/long-term care, school districts and other partners, subject to program guidance, eligibility, and funding availability.

Cybersecurity Protects Care Continuity

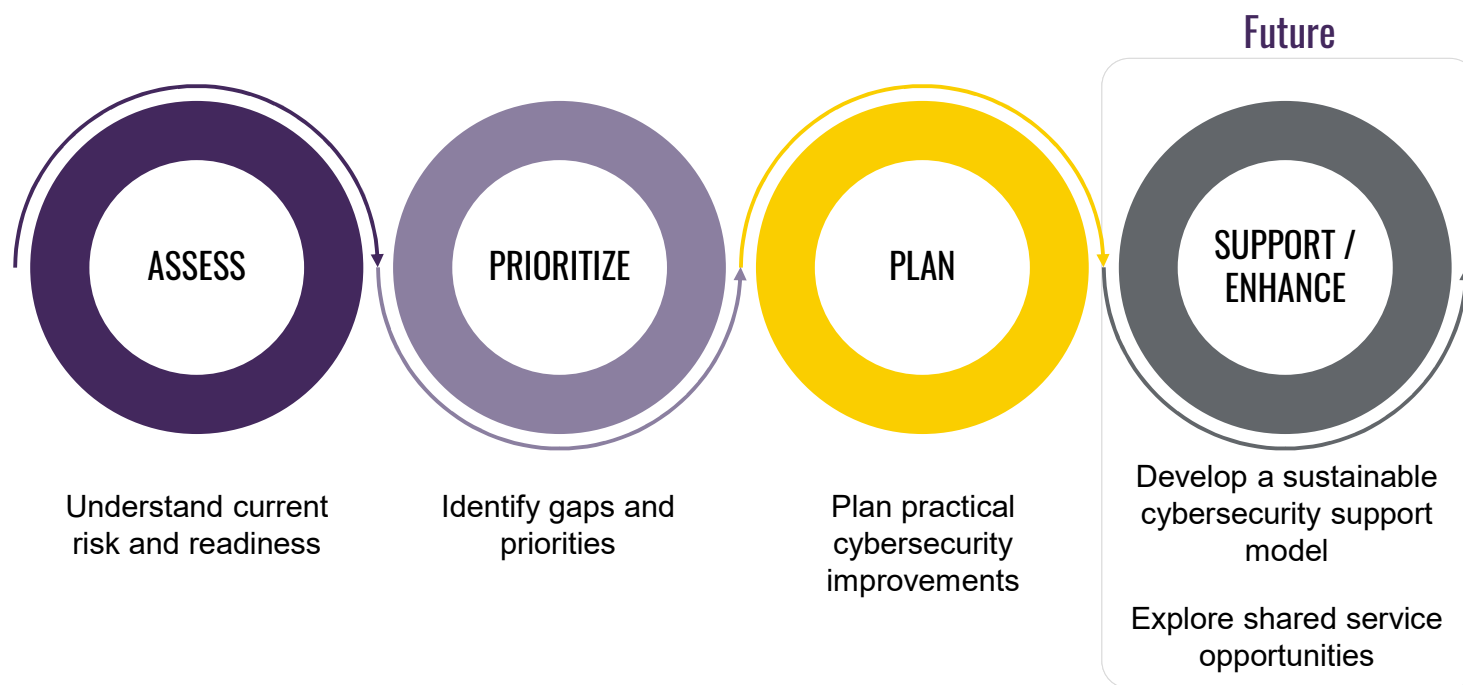
Cybersecurity is not only an IT issue. A cyber disruption can affect every part of rural health care.

Cybersecurity Resilience Initiative is designed to help rural facilities better understand **cyber risk** and **strengthen resilience** long term.



A Practical Path to Cybersecurity Resilience

Initiative 4 helps eligible facilities move from understanding their current state to planning for future improvements.



Completing a cybersecurity resilience assessment is the first step toward stronger resilience.

From Assessment to Action: What Happens Next

The cybersecurity resilience assessment establishes a baseline that helps determine next steps, foundational services, and future remediation planning.

1 Complete cybersecurity resilience assessment

ACTIVITY: Establish NIST CSF 2.0-aligned baseline per facility and determine common gaps across participating facilities.



ESTIMATED TIMING:
Aug–Nov 2026

2 Review results and confirm next steps

ACTIVITY: Assessment results help determine eligibility for foundational services and inform future RHTP cybersecurity-related funding consideration.

ESTIMATED TIMING:
After assessment completion

3 Access to foundational cybersecurity services

ACTIVITY: Facilities may access services such as:

- **Cyber Threat Intel Portal:** curated threat updates
- **Incident Response Retainer:** response planning support
- **Cybersecurity Learning Platform:** foundational training resources

ESTIMATED TIMING:
Following eligibility confirmation

4 Inform Phase 2 Risk remediation activities

ACTIVITY: Prioritize cyber risk remediation aligned with HHS Healthcare & Public Health Cybersecurity Performance Goals.

ESTIMATED TIMING:
Future phase

Completing the cybersecurity resilience assessment is required for facilities seeking future RHTP cybersecurity-related funding consideration. Future funding or support is subject to program eligibility, availability, NYSDOH guidance, and subject to CMS review and approval.

What Participation Looks Like

Participation is designed to be practical, guided, and collaborative from the start.



A simple interest form to confirm contacts and readiness



Follow-up to bring together the right facility participants



An opportunity to discuss questions or recent assessment work



Access to an easy-to-use web-based platform for the assessment process



Clear guidance on what information is needed and how to complete the assessment

The interest form is not the full assessment.

It will not include sensitive technical information, PHI, credentials, or detailed cybersecurity questions.

Assessment Outputs and Actionable Insights

Assessment responses can generate practical insights to support facility review and planning.



Assessment Outputs

- Progress and completion views
- Security posture reports and analytics
- Maturity insights
- Identified strengths and gaps
- Prioritized recommendations
- Inputs for future planning
- Projected improvements based on planned commitments (where applicable)
- Ability to track real-time maturity progress

How to Express Interest and Get Started

Facilities interested in participating should complete the Cybersecurity Resilience Interest Form by **August 31**. The form is used to coordinate the appropriate next step.



- Confirm the right facility contacts
- Understand interest and readiness
- Identify whether a recent assessment already exists
- Coordinate follow-up step

Questions?

Submit them in the Q&A. We'll answer a few live and use any remaining questions to inform the follow-up FAQ.

The form is not the full assessment. It should not include sensitive technical information, PHI, credentials, or detailed cybersecurity evidence.

Next Steps

After today's session, your facility can take a few simple steps to stay informed and move forward.

1

Review and share the presentation with the appropriate stakeholders.

2

Complete the Cybersecurity Resilience Interest Form by August 31 if your facility wants to participate.

3

Visit [NYSDOH RHTP website](#) for follow-up materials, including the webinar recording and FAQ.

4

Contact rhtpcyber@health.ny.gov with questions or to schedule a discussion before submitting the form.

Important: Completing the cybersecurity resilience assessment is required for facilities seeking future RHTP cybersecurity-related funding consideration. Future funding or support is subject to CMS review and approval, program eligibility, availability, and NYSDOH guidance.

THANK YOU

RHTPCyber@health.ny.gov