DRCHSD Summit

Delta Region Community Health Systems Development Program | 2023

DRCHSD Summit

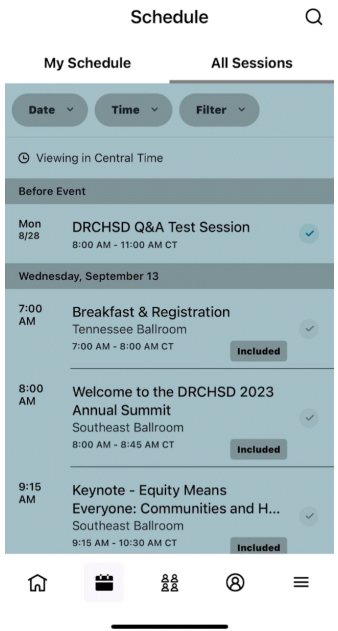
Delta Region Community Health Systems Development Program | 2023

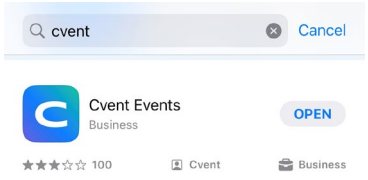
Defending Against Cyberthreats – Why You Need To and How You Can Do It On A Rural Budget

DRCHSD Summit

Delta Region Community Health Systems Development Program | 2023

Log-in to the CVENT app to participate in this sessions live Q&A.





Download the CVENT app

Open your phone camera and scan me!

Ask Yourself

- Are you performing annual security assessments?
- Do you have Healthcare Cyber Insurance?

1

Introductions

Introductions

Dr. Steve Pautler DPS MHA BSN FACHE, RHCEOC, CEO

Ste. Genevieve County Memorial Hospital

Judy Schmieder, RN, BSN

Director Clinical Informatics

Ste. Genevieve County Memorial Hospital

Monica Contreras, MBA, MHA

Director Digital Healthcare

Huron Consulting Group

Defending Against Cyberthreats

HURON

National Rural Health Resource Center

SGCMH

April 26, 2021

On this day, SGCMH and the rest of the world were focused on the Covid-19 pandemic.

SGCMH National Rural Health Resource Center

Timeline

April 26, 2021

Day 1

- MO **Homeland Security** sends **notification**
- Exchange **security patching deployed**
- Internet, external emails, & EHR **contained**, & **access shut down**

Day 2

- **Cyber Security insurance** vendor **notification** & **services initiated**
- Forced **password changes**

Day 7

- **Monitoring** deployed on **devices** and **servers**

Day 14

- **Email** system identified as **bigger threat**
- IT Ticketing System Server
- File Server

Day 15

- **Monitoring software** installed & **deployed** on hosted servers

Day 16

- **EHR limited access deployments** begin

Day 18

- **Server restored** w/access deployments ongoing
- PACS, rad, & EHR **interfaces restored**

Day 22

- Rebuilt & re-deployed **timekeeping** & **print server**
- **Lab interfaces** restored

Day 25

- **Med** & **supply dispensing** machines without threat & **interfaces restored**

Day 28

- **MFA** is setup & tested

Day 31

- **AV/MW** setup, testing, additional **issues** identified & corrected
- **Telemetry** & **fetal heart monitoring interfaces restored**

Day 32

- **Forms** interfaces & **PACS** web link **restored**
- **Forensics** showed AD credential dump was the only **exfiltration activity** noted

Day 35

- **Internet & EPrescribing restored**
- **MFA deployments start**
- **AV/MW** installed & **deployed**

Day 36

- **AV/MW** installed **on 90% of devices**

Day 63

- Bloomsdale Mid-America **VPN reconnected**

Day 77

- SGCMH Mid-America **VPN reconnected**

Day 78

- Radiology Spoke **Server re-installed**

Day 85

- **Patient Portal** email setup **restored**

Day 97

- Onsite **firewall upgraded**

Day 106

- **Shared** outlook **calendars restored**

Day 120

- Email to text **reminders reconfigured** on fax server
- Future clinic **text appointment** reminders working

Day 183

- **New ticketing system** implemented

Day 185

- **Single Sign-on multifactor authentication implemented**

Preparing for the unexpected

The Cost of Downtime

The average cost of IT downtime in healthcare is estimated at $5,600 - $9,000/minute with the average duration of downtime of 21 days with full recovery averaging 287 days.

According to HIPAA Journal, "347 healthcare data breaches of 500 or more records were reported to the Department of Health and Human Services' Office for Civil Rights" in the first half of 2022 alone

2013, Advocate Medical Group
- Cost: **$5.6M**
- People affected: **4M**
- **Theft**

2013, Excellus Health Plan, Inc.
- Cost: **$17M**
- People affected: **10M**
- **Hacking**

2014, Community Health Systems
- Cost: **$3.1M**
- People affected: **4.5M**
- **Hacking**

2015, Medical Informatics Engineering
- Cost: **$1M**
- People affected: **3.9M**
- **Hacking**

2014, University of California, LA Health
- Cost: **$7.5M** class-action lawsuit
- People affected: **4.5M**
- **Hacking**

2016, Banner Health
- Cost: **$6M**
- People affected: **3.6M**
- **Hacking**

2015, Anthem (formerly WellPoint)
- Cost: **$117M** to resolve litigation
- People affected: **78.8M**
- **Hacking**

2018, American Medical Collection Agency
- Cost: **$21M**
- People affected: at least **21M**
- **Hacking**

2014, Premera Blue Cross
- Cost: **$74M** class-action settlement
- People affected: **11M**
- **Hacking**

2020, Trinity Health
- People affected: **3.2M**
- **Hacking**

2022, Advocate Aurora Health
- People affected: **3M**
- **Impermissible Exposure**

2022, Shields Health Care Group
- People affected: **2M**
- **Hacking**

(multisources)

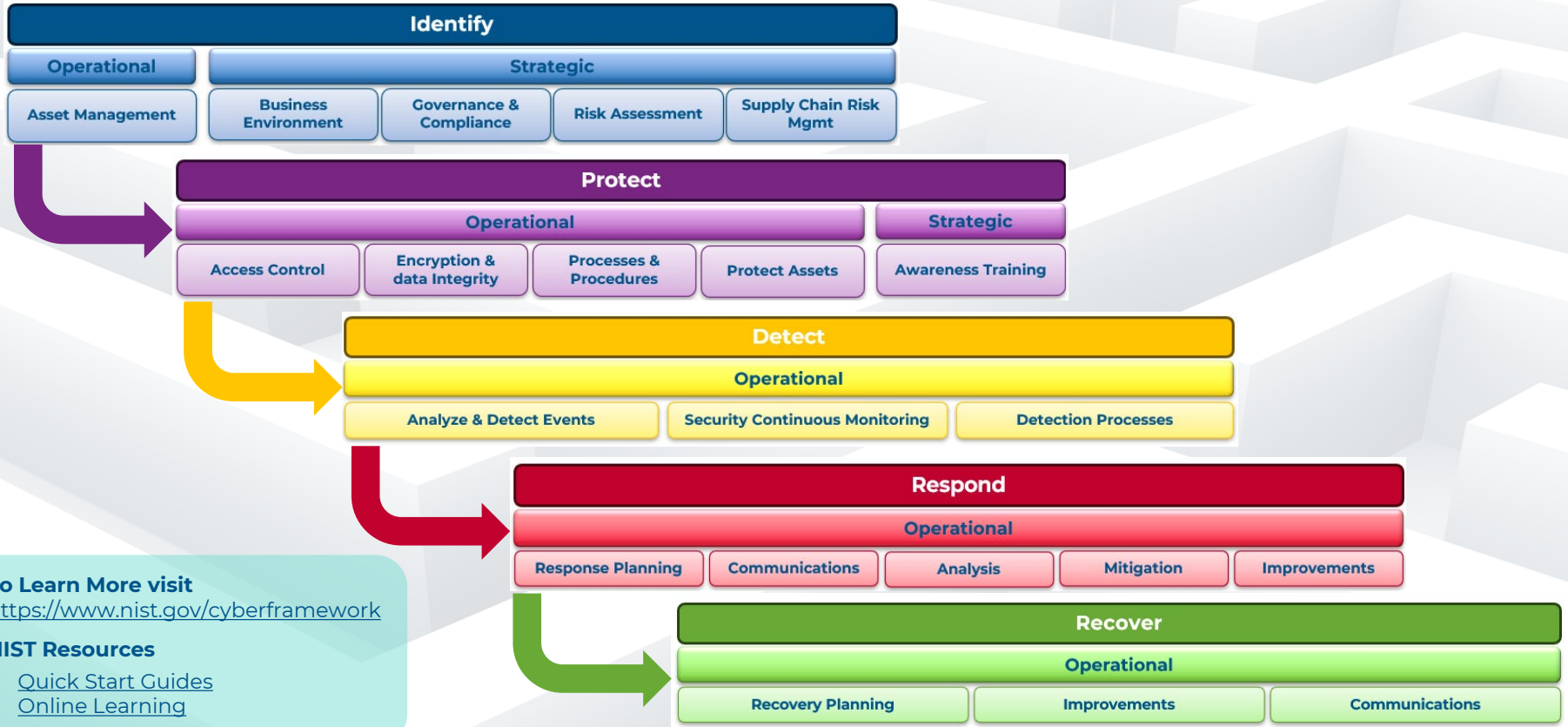
Loss of Productivity	Non-compliance fines and penalties	Equipment	Post-incident activities	Recovery	Detection	Lost Revenue	Business Disruption

SGCMH National Rural Health Resource Center

2

What you need to know to develop your Action Plan

NIST Cybersecurity Framework



To Learn More visit
https://www.nist.gov/cyberframework

NIST Resources

- Quick Start Guides
- Online Learning

SGCMH National Rural Health Resource Center

Disaster Recovery & Business Continuity

Application recovery occurs only **after** the critical IT infrastructure is setup and operational

Priority #1 - Critical IT Infrastructure

- Phone lines & Router
- Phone system
- Internet
- SAN & controller
- Physical equipment

The base infrastructure and services required to restore mission and business functions

Priority #2 - Mission Critical Applications

- EHRs & Interface Engine
- PACS, Med Dispensing Machine
- Office365
- NurseCall

Clinical care functions with the greatest impact on patient care requiring immediate recovery are categorized and ranked as Mission Critical

Priority #3 - Business Critical Applications

- Revenue-focused functions

Does not meet criteria of mission critical but needs to be brought up soon after

Priority #4 - Important Applications

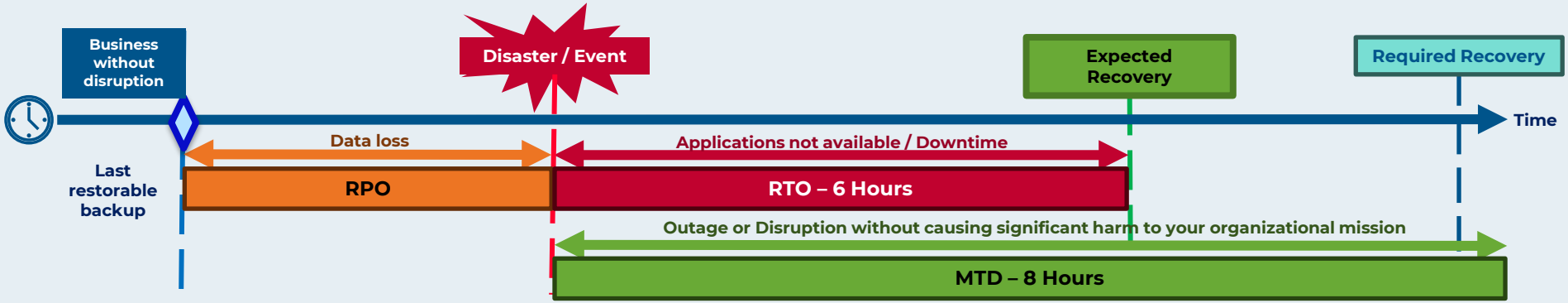
- All other applications

Priority #5 - Deferrable Applications

- Budgeting
- Training
- Low-impact activities

Disaster Recovery Metrics

RPO, RTO, and MTD



Recovery Point Objective (RPO)
RPO dictates backup frequency

Goal: Backup data to be as current as possible to lessen data loss risks (perm or temp).

- **How much data loss projected**
- **Max amt. of data loss tolerated**
- **Cost of lost data**
- **Cost to re-enter lost data**
- **Solution implementation costs**

Recovery Time Objective (RTO)
Timeframe Recovery Team must fully recover from event

Faster (30-min) RTOs result in **higher costs**

- **Project loss in revenue if system is in accessible**
- **Does the system handle patient data?**
  - **Consider Patient SLAs**
  - **Consider Customer/Department SLAs**
- **What dependencies exist**
- **Other systems impacted (inc. RTOs)**
- **Patient-facing systems or apps resulting in dissatisfaction (portal)**

Maximum Tolerable Downtime (MTD)

The total amount of acceptable for mission / business process outage or disruption – including all impact considerations.

SGCMH National Rural Health Resource Center

Critical Hardware & Application Inventories

Complete Business Impact Analysis (**BIA**) to predict consequences of disruption to develop recovery strategies

Create an **Action Plan** designed to provide visibility to your technology portfolio and include internal Point of Contact (POC) and vendor support contact information to assist in a **streamlined recovery process**

Priority	Rank	BIA Document	BIA POC	System Function
1	1.a	Network	Network Administrator	Phone Lines
1	1.a	Network	Network Administrator	Internet
1	1.a	Network	Network Administrator	Phone System
1	1.b	Network	Network Administrator	Network
1	1.b	Network	Network Administrator	Active Directory
1	1.b	Network	Network Administrator	Imprivata
1	1.b	Network	Network Administrator	SAN (Controller)
1	1.b	Network	Network Administrator	SAN
1	1.c	Network	Network Administrator	Print Servers
1	1.c	Network	Network Administrator	Active Directory
1	1.c	Network	Network Administrator	Fax Server
1	1.c	Network	Network Administrator	SQL Server
1	1.Cloud	Network	Network Administrator	File Servers
1	1.Cloud	Network	Network Administrator	Active Directory
1	1.Cloud	Network	Network Administrator	Print Servers
1	1.d	Network	Network Administrator	File Servers
1	1.d	Network	Network Administrator	Intranet
1	1.e	Network	Network Administrator	Ironport

Disaster Recovery Initiation of Plan

The Disaster Recovery team is focused on planning, implementing, maintaining, auditing, and testing an organization's procedures for business continuity and recovery.

Disaster / Incident Occurs

Who are the **Emergency Facilitators** and what's next**?**

Plan Initiation Checklist:

- ✓ IT Leadership receives notification of existing outage / emergency
- ✓ IT Leadership notifies Executive team
- ✓ Degree of disaster determined
- ✓ IT Leadership in conjunction with Executive member activate proper application recovery plan dependent on extent of disaster
- ✓ Locate Critical Application Plan
- ✓ Notify end users of the disruption of service
- ✓ Contact backup site and establish schedules
- ✓ Contact all other necessary personnel–both user and data processing
- ✓ Contact vendors–both hardware and software
- ✓ Monitor progress

Network Disaster Recovery Manager (NDRM)

- **Activates** the network **disaster recovery plan**
- **Call** network recovery resources **to action**
- **Directs** the network recovery activities
- **Activates** the command center

Name of NDRM
Phone Number

Business Continuity Coordinator (BCC)

- **Initiates** contact with **Recovery Team**
- **Designates** team members to notify departments
- **Manages** communication
- **Call** key recovery resources **to action**

Name of BCC
Phone Number

SGCMH National Rural Health Resource Center

Recommended Update & Review Practice

Clinicians always need access to patient data and when faced with a disaster, it is critical to get back in business quickly with accurate and updated patient records. You should review plans for all critical operations as needed or every six (6) months and all other plans annually.

Update DRBC Plans with organizational changes

Supplement your DRP with security/data protection solutions

Maintain a disaster recovery playbook

Formalize & implement "Incident Report" & "Checklist" templates provided

Perform realistic testing scenarios & develop a comprehensive post-testing report

Perform annual updates for downtime policies, procedures, and plans

Keep full copies of critical data offsite and located >150 miles away from primary data center

Compliance & Governance

- National Institute of Standards and Technology (**NIST**)
- Payment Card Industry (**PCI**)
- Health Insurance Portability & Accountability Act (**HIPAA**)
- General Data Protection Regulation (**GDPR**)
- New York Department of Financial Services (**NYDFS**)
- Health Information Technology for Economic & Clinical Health Act (**HITECH**)

Backup Data

- Follow 3-2-1 backup rule
- Increase frequency of backups
- Align backups & service-level demands
- Protect endpoints & SaaS apps
- Automate disaster recovery
- Cloud backup

Security Tools

- Network Security
- Packet Sniffers
- Encryption
- Antivirus Software
- Managed Detection
- Firewall
- PKI Services
- Network Defense Wireless
- Vulnerability Scanning
- Penetration Testing

Strengthening Your Cybersecurity Posture

Protect against potential cyberattacks

Multi-Factor Authentication

- Multiple methods of authentication
- Verify user's identity
- Reduce risks of compromised passwords

Educate & Train Employees

- Teach about cyber threats and accountability
- Train on proper email use
- Prioritize and establish protocol
- Ensure employees understand their role
- Formal written security policies

Cloud Services

- Mitigate risks
- Improve Disaster Recovery
- Trusted Experts
- Automate continuously monitoring
- Centralize patching, testing, & auditing

Questions?

Thank you!

Appendix

Testing
Scenarios
Examples

Checklist for Testing DR Plan

There are common accepted ways to perform DR testing. Tabletop run-through walks your team through the plan as if were being executed.

- How will you notify your workforce about the incident?
- Who is expected to come in the office and who can work remotely?
- Which departments are affected the most and need immediate relief?
- Do you have a backup power generator? Do you have a designated resource who can operate equipment?
- Do you have an arranged office or mobile recovery location

Scenario Testing – Power Outage

There is a power outage due to a recent storm and the utility company reports power will not be restored for a few days. What do you do?

- How will you notify your workforce about the incident?
- Who is expected to come in the office and who can work remotely?
- Which departments are affected the most and need immediate relief?
- Do you have a backup power generator? Do you have a designated resource who can operate equipment?
- Do you have an arranged office or mobile recovery location

Scenario Testing – Network Outage

Power outages inevitably lead to network outages. However, network outages can occur without a power outage.

- Does everyone have access to their work systems?
- Is everyone aware of the security measures to take while working remotely?
- What is the plan for network restoration?

Scenario Testing – Physical Disruption

Natural disasters or other critical situations (e.g., active shooter, bomb threat, etc.) can cause disruption and require emergency procedures and safety steps.

- Are there technology areas not protected by additional security measures? Who has access to the IT department and resources? *Keep in mind this is technology focused.*
- Which departments are affected the most and need immediate relief?
- Are you able to communicate during a disaster or an emergency? What are your alternative means of communication?

Potential Scenarios

Determine how realistic and detailed scenarios should be for testing. Tabletop testing is a plan review where employees participate to confirm everyone knows their responsibilities in various emergencies.

Scenario	Description	Importance
Disgruntled employee sabotages a critical system functionality	Although infrequent, these events are possible, especially where security may be lax (e.g., lack of secured access to critical technology area/department)	Someone who is familiar with your technology and processes may, over time, identify a potential weakness in equipment or technology
Employee enters/edits/changes critical process data incorrectly, fails to validate entry causing a massive outage	Accuracy and care are required criteria in any technology-controlled environment	Improper changes is a potential problem and may be necessary to build additional security challenges and checkpoints to minimize errors
Employee returns to work and contaminates other employees with an airborne human-to-human virus that sickens half of the staff	Difficult to address when signs and symptoms are not present when returning to work from a day off or the weekend	Concerns about epidemics and pandemics should be addressed in DRBC plans because of the staffing impact
A member of IT uses access privileges to steal intellectual property and sell it to competing organizations	Again, this scenario is infrequent, but any employee can “go rogue” and use access to steal information	Employee-based situations should be factored into DRBC plans and exercises, not just involving a loss of technology or disaster

Scenario Testing – Cyber Event

Your organization receives initial notification that computer systems / email are vulnerable. After monitoring software is deployed on devices and servers a larger threat is identified requiring extensive action to be taken.

Action	Owner
• Who receives notification from MO Homeland Security? • Who is the backup when Primary Resource is not available?	
Activate network **disaster recovery plan** & contact **business continuity coordinator (BCC).**	
Call network resources to action	
BCC Initiates call to action for the **recovery team** and manages communication plan ongoing. Establish frequency and method to communicate to internal and external resources.	
Required communicate to external resources:	
• Determining what services or hardware is impacted and required to be offline? • Who approves decision to take down technology services?	
Activate downtime plans reviewed with departments	
Departments are notified when services are restored for their area through the communication coordinator. What's next?	
Complete **post-incident analysis** and **document recommendations** and **corrective actions**.	
Obtain incident report approval from administration.	

Scope of Work

National Rural Health Resource Center *engaged Huron Consulting Group to facilitate and provide deep expertise in Security Management and development of a Disaster Recovery / Business Continuity Plan (DR/BCP).*

Planning activities included:

- Assemble Plan
- Identify Scope
- Appoint Emergency Contacts
- Designate Disaster Recovery Team
- Assign Roles & Responsibilities
- Data & Backup Locations
- Restore Technology Functionality
- Security & Risk Assessment
- Business Impact Analysis
- Recovery Strategies
- Solution Implementation
- Training, Acceptance, & Maintenance

This project is supported by the Health Resources and Services Administration (HRSA) of the U.S. Department of Health and Human Services (HHS) as part of a financial assistance award totaling $10,000,000 with 100% funded by HRSA/HHS and $0 amount and 0% funded by non-government sources. The contents are those of the author(s) and do not necessarily represent the official views of, nor an endorsement by HRSA/HHS, or the U.S. Government.

References

- https://healthitsecurity.com/news/2-million-individuals-impacted-by-shields-health-care-group-cyberattack
- https://www.wpr.org/data-breach-advocate-aurora-health-system-may-have-exposed-3m-patients-information
- https://www.paubox.com/resources/over-half-million-trinity-health-patients-affected-data-breach/
- https://www.hipaajournal.com/banner-health-agrees-to-pay-6-million-to-settle-data-breach-lawsuit/
- https://www.netsec.news/medical-informatics-engineering-settles-hipaa-violation-cases-for-1-million/
- https://www.healthcarefinancenews.com/news/advocate-health-care-agrees-55-million-hipaa-violation-settlement
- https://www.bankinfosecurity.com/settlement-reached-in-community-health-systems-breach-suit-a-12001
- https://www.latimes.com/business/la-fi-ucla-medical-data-20150717-story.html
- https://www.hipaajournal.com/cost-of-the-excellus-bluecross-blueshield-data-breach-3338/
- https://www.govtech.com/security/premera-blue-cross-to-pay-74m-over-data-breach.html
- https://www.attorneygeneral.gov/taking-action/ag-shapiro-announces-multistate-settlement-with-american-medical-collection-agency-over-2019-data-breach/#:~:text=As%20part%20of%20the%20settlement,terms%20of%20the%20settlement%20agreement.
- https://www.reuters.com/article/us-anthem-cyber-settlement/anthem-to-pay-record-115-million-to-settle-u-s-lawsuits-over-data-breach-idUSKBN19E2ML
- https://www.hipaajournal.com/consolidated-class-action-shields-health-care-group/
- Securing Critical Infrastructure: Building Resilience | Committee for Economic Development of The Conference Board (ced.org)
- Cybersecurity for Small Businesses | Federal Communications Commission (fcc.gov)

SGCMH National Rural Health Resource Center