Chris Ramos, Cybersecurity State Coordinator

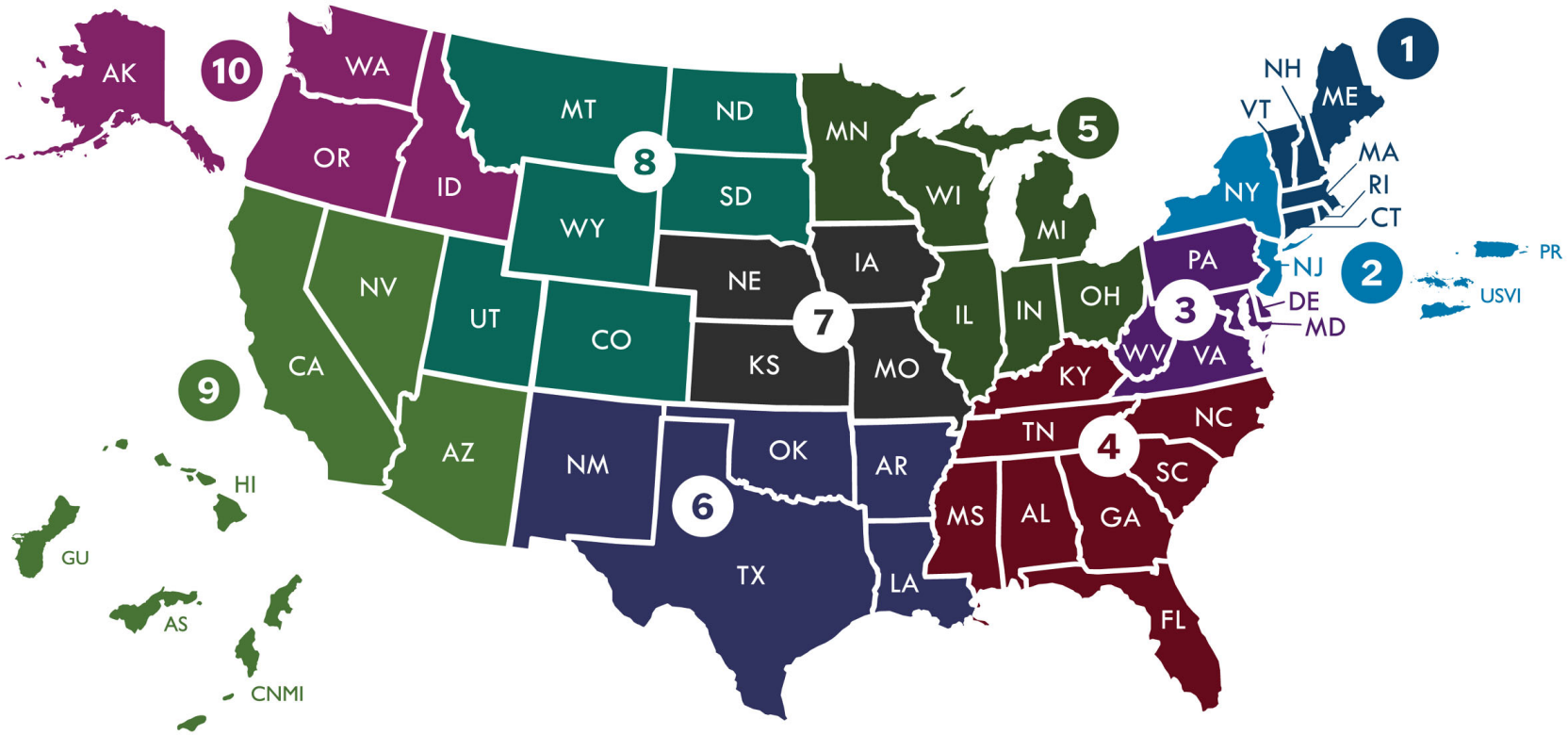
CISA | CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

As America's Cyber Defense Agency and the National Coordinator for critical infrastructure resiliency and security, CISA leads the national effort to understand, manage, and reduce risk to the cyber and physical infrastructure that Americans rely on every hour of every day.

CISA Regions

- 1 Boston, MA
- 2 New York, NY
- 3 Philadelphia, PA
- 4 Atlanta, GA
- 5 Chicago, IL
- 6 Dallas, TX
- 7 Kansas City, MO
- 8 Denver, CO
- 9 Oakland, CA
- 10 Seattle, WA



CISA.GOV/REGIONS

2023 Ransomware Attack Against Healthcare System

CT INSIDER

Subscribe Sign in

JOURNAL INQUIRER

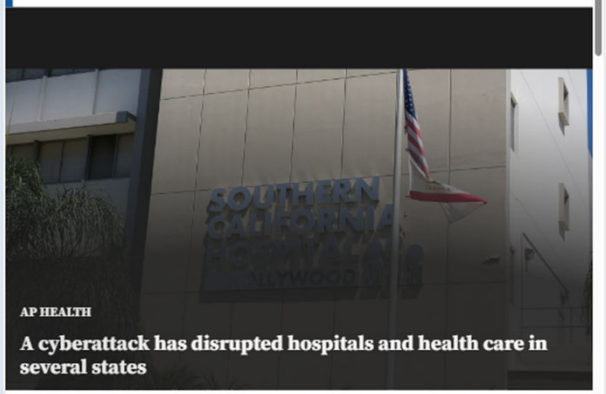
International extortion group claims to have confidential information in month-long cyber attack on CT hospitals

By Eric Bedner, Staff Writer
Aug 30, 2023

Rockville General Hospital on Friday, August 4, 2023, in Manchester.
Jim Michaud / Hearst Connecticut Media

44° abc7.com

WEATHER ALERT
There are 5 areas with 5 active weather alerts. >



AP HEALTH

A cyberattack has disrupted hospitals and health care in several states

The Southern California Hospital at Hollywood is seen in the Hollywood district of Los Angeles on Friday, Aug. 4, 2023. The Southern California Hospital at Hollywood is seen in the Hollywood district of Los Angeles on Friday, Aug. 4, 2023. Hospitals, including this one ...

Read More

by: PAT EATON-ROBB, Associated Press
Posted: Aug 4, 2023 / 06:35 PM MDT
Updated: Aug 4, 2023 / 06:37 PM MDT

SHARE

This is an archived article and the information in the article may be outdated. Please look at the time stamp on the story to see when it was last updated.

MANCHESTER, Conn. (AP) — Hospitals and clinics in several states on Friday began the time-consuming process of recovering from a cyberattack that disrupted their computer systems, forcing some emergency rooms to shut down and ambulances to be diverted.

Many primary care services at facilities run by Prospect Medical Holdings remained closed on Friday as security experts worked to determine the extent of the problem and resolve it.

John Riggi, the American Hospital Association's national advisory for cybersecurity and risk, said the recovery process can often take weeks, with hospitals in the meantime reverting to paper systems and

THE HIPAA JOURNAL

The HIPAA Journal is the leading provider of news, updates, and independent advice for HIPAA compliance

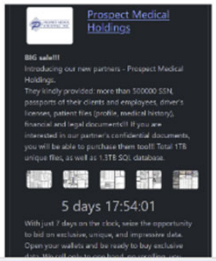
Become HIPAA Compliant » HIPAA News » HIPAA Compliance Checklist Latest HIPAA Updates »
HIPAA Training » About Us »

Medical Records from Prospect Ransomware Attack Appear on Dark Web

Posted By Steve Alder on Aug 29, 2023

Medical records extracted during the recent Prospect Medical Holdings ransomware attack are being allegedly offered for sale on the dark web according to social media sources. The notification of the sale has been interpreted as a signal to Prospect Medical Holdings to quickly respond to the hackers' ransom demands.

On August 3, the Prospect Medical Holdings health system was hit by a ransomware attack that crippled operations at the health system's 17 hospitals and 166 outpatient clinics. At the time, the perpetrators of the attack were unknown. However, last week, a notice appeared on the Rhysida dark leak site, claiming responsibility for the attack.



The notice also announced an auction of data hacked in the attack – the data consisting of more than 500,000 Social Security Numbers, passports of clients and employees, drivers' licenses, patient files (profiles and medical histories), financial and legal documents. In all, it is claimed, the sale consists of 1TB of unique files and a 1.3TB SQL database.

The notice was accompanied by several snapshots of the stolen data – some of which has been independently verified as genuine by

Working with CISA: Voluntary & No-Cost Cybersecurity Offerings

- **Assessments & Evaluations**
  - Cybersecurity Performance Goals
  - Ransomware Readiness Assessment
  - Cyber Resilience Reviews
  - Vulnerability Scanning & Web Application Scanning
  - Risk and Vulnerability Assessments (aka “Pen” Tests)
  - External Dependencies Management Reviews
  - Cyber Security Evaluation Tool (CSET™)
  - Validated Architecture Design Review (VADR)

- **Preparedness Activities**
  - Cybersecurity Alerts & Advisories
  - Information / Threat Indicator Sharing
  - Cybersecurity Training and Awareness
  - Cyber, Physical, Convergence Tabletop Exercises and “Playbooks”
  - National Cyber Awareness System
  - Vulnerability Notes Database
  - Information Products and Recommended Practices
  - Workshops (Cyber Resilience, Cyber Incident Management, Election Security, etc.)

- **Partnership Development**
  - Informational Exchanges
  - Working Group Support
  - Joint Cyber Defense Collaborative (JCDC)

- **Strategic Messaging & Advisement**
  - Resource Briefings
  - Keynotes and Panels
  - Threat Briefings
  - Topic Specifics (e.g., CAM, SCRM, ICS, etc.)

- **Incident Response Assistance**
  - Remote / On-Site Assistance
  - Malware Next-Generation Analysis
  - Hunt and Incident Response Teams
  - Incident Coordination
  - Targeted (Victim) Notifications

Reference: https://www.cisa.gov/cyber-resource-hub

Healthcare and Public Health Sector Preparedness Resources

- Healthcare and Public Health Toolkit (https://www.cisa.gov/topics/cybersecurity-best-practices/healthcare)
- HHS Administration for Strategic Preparedness and Response (ASPR) Technical Resources, Assistance Center & Information Exchange (TRACIE) Resources
  - Technical Resources Page (https://asprtracie.hhs.gov/technical-resources)
  - Healthcare System Cybersecurity: Readiness and Response Considerations (https://files.asprtracie.hhs.gov/documents/aspr-tracie-healthcare-system-cybersercurity-readiness-response.pdf)
  - Healthcare System Cybersecurity Response: Experiences and Considerations Webinar (https://files.asprtracie.hhs.gov/documents/cybersecurity-response-experiences-and-considerations-webinar-final.pdf)
- Critical Infrastructure Protection (CIP) Cybersecurity Weekly Bulletin Signup (https://www.phe.gov/Preparedness/planning/cip/Pages/CIPInquiry.aspx) (contact: CIP@hhs.gov)
- HHS Health Sector Cybersecurity Coordination Center (HC3) (https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html) (contact: HC3@hhs.gov)
- HHS 405(d): Aligning Healthcare Security Approaches (https://405d.hhs.gov/information) (contact: Cisa405d@hhs.gov)
- HPH Cybersecurity Framework Implementation Guide (https://aspr.hhs.gov/cip/hph-cybersecurity-framework-implementation-guide/Pages/default.aspx)
- Healthcare Sector Coordinating Council (HSCC) Recommended Cybersecurity Practices (https://healthsectorcouncil.org/hscc-publications/)
- Ransomware:
  - CISA Stop Ransomware Website: HPH Sector (https://www.cisa.gov/stopransomware/healthcare-and-public-health-sector)
  - CISA Stop Ransomware Guide (https://www.cisa.gov/resources-tools/resources/stopransomware-guide)
  - Protecting Against Ransomware (https://www.cisa.gov/news-events/news/protecting-against-ransomware)

CISA Campaigns

Shields Up

As the nation's cyber defense agency, CISA stands ready to help organizations prepare for, respond to, and mitigate the impact of cyberattacks. Visit https://www.cisa.gov/shields-up to learn more.

Shields Ready

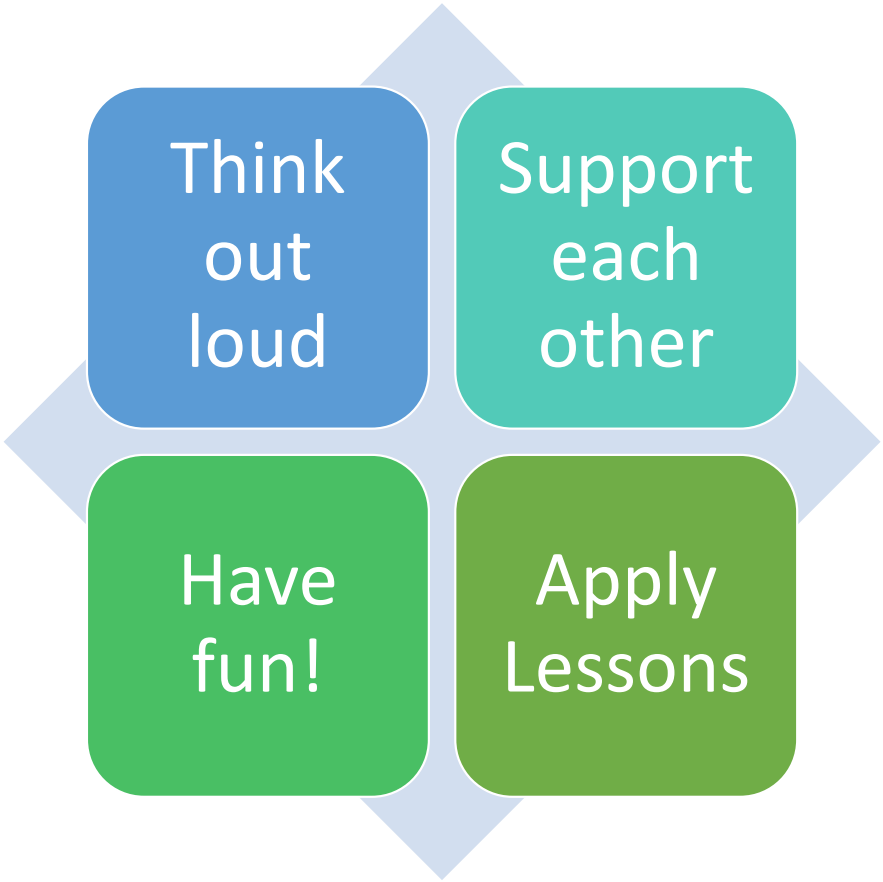
As the National Coordinator for critical infrastructure security and resilience, CISA stands ready to help America prepare for and adapt to changing risk conditions and withstand and recover rapidly from potential disruptions, regardless of cause. Visit https://www.cisa.gov/shields-ready to learn more.

Artificial Intelligence

As the nation's cyber defense agency and the national coordinator for critical infrastructure security and resilience, CISA will play a key role in addressing and managing risks at the nexus of AI, cybersecurity, and critical infrastructure. Visit https://www.cisa.gov/ai to learn more.

Reference: https://www.cisa.gov/spotlight

Tabletop Exercise Tips



Chris Ramos
Cybersecurity State Coordinator
Email: Christoper.Ramos@cisa.dhs.gov
Phone: (202) 316-6440

Report Cyber Issues 24/7
Email: central@cisa.dhs.gov
Phone: (888) 282-0870
Website: https://www.cisa.gov/

For more information, visit **CISA.gov** or contact **central@cisa.dhs.gov**