

Not Just An IT Issue


Lisa Fenger
May 21, 2024



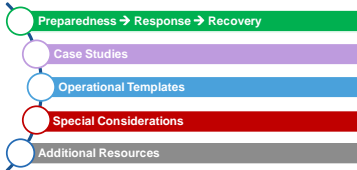
GREATER NEW YORK HOSPITAL ASSOCIATION
Over 100 years of helping hospitals deliver the finest patient care in the most cost-effective way.

1

2 Cyber Disruption Toolkit Overview




Goal: Managing consequences from a cyber disruption and continuing operations and patient care throughout downtime



2

3 Agenda



- GNYHA Overview
- Cybersecurity Background
- Exercise Overview
- Results
- Conclusions

3

Greater New York Hospital Association

Overview

4

5 Greater New York Hospital Association

- Trade association based in New York City
- Hospitals
 - Nearly 160 member hospitals and health systems
 - Members are located in metropolitan New York, throughout New York State, and in New Jersey, Connecticut, and Rhode Island
- Provide advocacy for members



5

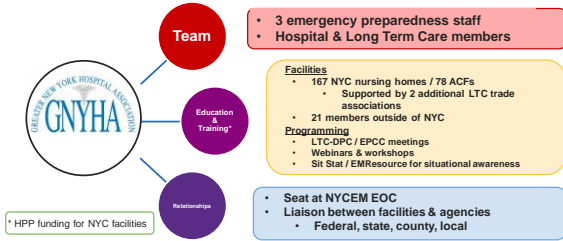
6 Greater New York Hospital Association

- Continuing Care
- 57 members
 - Not-for-profit and public organizations
 - Located in NYC, Long Island and Westchester County
 - Members provide short- and long-term skilled nursing, rehabilitation services, home health care, palliative care, adult day care, senior housing, independent living, assisted living, dialysis services



6

7 Emergency Preparedness and Response at GNYHA



7



8

9 Cybersecurity Statistics



Through mid-2023

- 327 data breaches had been reported to HHS's Office for Civil Rights
- Up more than 104% from 160 breaches as of mid-2022
- Costs: average of \$10 million per breach

Affected data: 40 to 89 million individual patients

- 60% increase year-over-year for the first six months.
- 2022: single breach involved 2 million records
- First half of 2023: 5 breaches of at least 3 million records each

9

10 Why Healthcare



- Access to data through third party vendors
- Lack of network security
- Physical theft
- Use of legacy systems
- Sensitive and valuable data

10

11 Why Is the Data Valuable



- Personal and medical information is sold
 - Health records are permanent
 - Exposes private medical and personal information
- Passwords can be used to commit fraud and identity theft
 - Submit claims for false medical treatments
- Data can be held for ransom payments
 - Threatens patient health
 - Threatens business operations
 - Even without paying ransom, it costs the organization



11

12 2019 Ransomware Attack: Wisconsin



Wisconsin nursing home provider

- Cloud data hosting
- 110 nursing homes affected
- Cost: \$14 million

Critical business functions interrupted:

- Electronic billing
- Payroll management
- Internet and email services

Patient care: pen and paper records

12

13 2022 Ransomware Attack: Consulate Health Care

Suspicious computer network activity

- + Access apparently through a vendor's system
- + 140 nursing homes

Critical information affected:

- + Business functions: budgets, plans, corporate structure
- + Employee information: SSNs, emails, photos, contact info, insurance info
- + Customer information: SSNs, credit cards, emails, medical records

<p>Hacker claims</p> <ul style="list-style-type: none"> + Stole 550 GB of data + Could release the information 	<p>Consulate response</p> <ul style="list-style-type: none"> + Can't afford ransom + Cyber insurance won't cover ransom just response costs
---	--

13

14 2024: Our Fragile Healthcare System

February 21: Change Healthcare

- ☐ Ransomware attack
- ☐ Potentially impacting 1/3 of US healthcare patients
- ☐ Not an attack on a facility: an attack on healthcare transactions
- ☐ Affected hospitals and pharmacies

Impact: widespread repercussions across the industry

May 8: Ascension

- ☐ Ransomware attack
- ☐ Affecting 140 hospitals in multiple states
 - ☐ Ambulance diversions
 - ☐ Long term care facilities
 - ☐ Pharmacies
- ☐ Facilities resorting to pen and paper downtime procedures

Impact: direct disruption of ability to provide patient care

14

15 2018 New York City Public Health Jurisdictional Risk Assessment

- The following lists show hazards that are most severe, most likely, and best able to be managed by the City in descending order (09 to lowest, where 1 is most serious):
- | | | |
|--|--|--|
| <p>Most severe</p> <ol style="list-style-type: none"> 1. Respiratory virus with pandemic potential 2. Water contamination 3. Chemical release 4. Chemical release 5. Emerging disease with pandemic potential 6. Disease outbreak 7. Emerging disease with pandemic potential 8. Air contamination 9. Mass casualty incident | <p>Most likely</p> <ol style="list-style-type: none"> 1. Cyberattack 2. Mass casualty incident 3. Emerging disease with pandemic potential 4. Respiratory virus with pandemic potential 5. Chemical release 6. Air contamination 7. Water contamination 8. Chemical release 9. Cyberattack | <p>Best able to be managed by the City</p> <ol style="list-style-type: none"> 1. Radiation hazard 2. Coastal erosion 3. Mass casualty incident 4. Emerging disease with pandemic potential 5. Respiratory virus with pandemic potential 6. Water contamination 7. Chemical emergency 8. Chemical release 9. Chemical release |
|--|--|--|









The Role of Public Health Division in New York City, The 2018 New York City Public Health Jurisdictional Risk Assessment Report

15

Exercise Overview

16

17 Exercise Scope

 Facilitated TTX	 Virtual
 3 hours	 2 vignettes
 3 times, 2 days	 10 breakouts

17

18 Exercise Objectives

- 1 Examine the plans and abilities of NYC long-term care facilities to respond to a significant cyber incident.
- 2 Evaluate the ability for the NYC long-term care facilities to gather and disseminate essential elements of information during a significant cyber incident.
- 3 Explore processes for requesting incident response resources.
- 4 Explore NYC long-term care facilities' processes for internal and external messaging during a cyber incident.
- 5 Discuss members' plans, processes, and procedures for recovering from a significant cyber incident.

18

19 Exercise Summary: Scenario





- **Vignette 1:** A distributed denial of service attack and data exfiltration incident impacting patient health information and personally identifiable information.
- **Vignette 2:** A compromise to participants' EMR vendor(s) that resulted in data manipulation and ransomware on their facility's systems and devices.



19

20 Exercise Participation








Facilities	Agencies	Organizations
68 nursing homes  4 adult care facilities 	<u>Local</u> <ul style="list-style-type: none"> • NYC DOHMH • NYCEM • NYPD • NYC Cyber Command <u>State</u> <ul style="list-style-type: none"> • NYS Dept of Health <u>Federal</u> <ul style="list-style-type: none"> • CISA • FBI 	<u>Associations</u> <ul style="list-style-type: none"> • GNYHA • GNYRCFA • SNYA <u>Other</u> <ul style="list-style-type: none"> • Healthix • IMS • Centers Health Care

20

Results

21

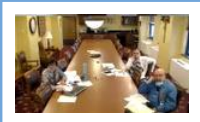
22 Observations

-  Cyber incidence preparedness guidance
-  Cyber incidence reporting requirements
-  Cybersecurity training for staff
-  Medical record access if EMRs are offline
-  Communication plan improvement

22

23 Results: Areas of Strength

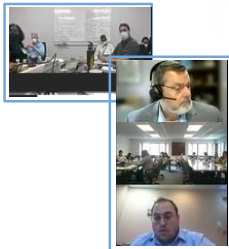
- **Teamwork & partnership across the sector/network**
- "Right team members in the room"
- Identified needs (e.g., cyber training, incident response plans, backups, etc.)
- Recognized priorities for the organization during an incident
- Preparation for EMR disruptions
- Policies
- Practicing / drills / exercises



23

24 Results: Areas of Improvement

- **Talk with leadership**
- Cyber training and education
- Understand, identify, and address vulnerabilities
- Build relationships with external partners before an incident
- More backup/downtime plans and processes
- Improve communications capabilities (e.g., pre-written messages and contact info)
- Develop or improve incident response plan or documentation for a cyber incident

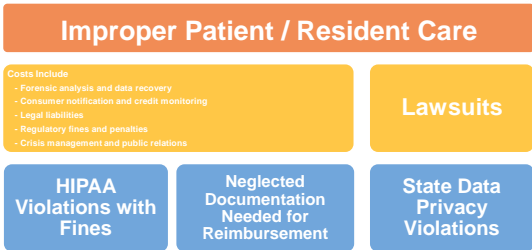


24

Conclusions

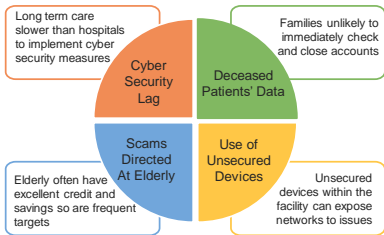
25

26 Implications



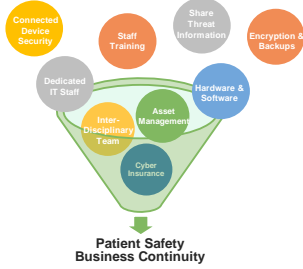
26

27 Long Term Care Vulnerabilities

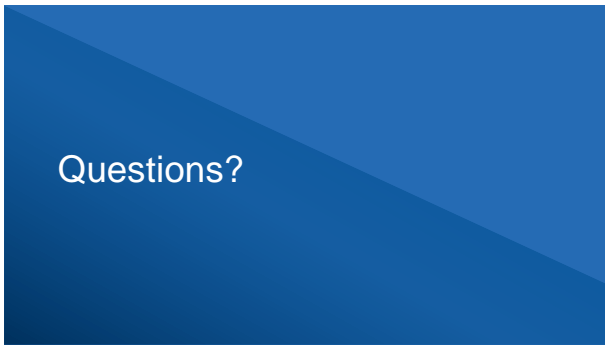


27

28 Cyber Preparedness



28



29

30 Thank you!



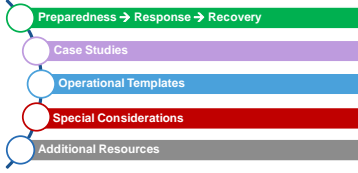
Lisa Fenger
 Assistant Director
 Emergency Preparedness & Response
 Greater New York Hospital Association
lfenger@gnyha.org
 212-506-5432 office
 347-501-2802 cell

30

31 Cyber Disruption Toolkit Overview



Goal: Managing consequences from a cyber disruption and continuing operations and patient care throughout downtime



31