# WELCOME

**GINA GAMBARO**

Director of Marketing

# Asking a question is easy!

- **About the topic being presented** —
  - Click on the **Q&A** icon at the bottom of your screen
  - Type your question & hit Enter
  - Questions will be answered at the program's end, or offline if time runs out
- **About technical issues or CE credit** —
  - Click on the **Chat** icon at the bottom of your screen
  - Type your question & hit Enter
  - Our team will reply to your question right away

# Housekeeping notes

- This webinar is being recorded for on-demand access later, after the series' conclusion
- To earn CE, you must attend the entire session
- **For those sharing a computer**
  - Complete a manual sign-in sheet before the program ends
  - Go to **Chat** to access the link for the sign-in sheet
  - Each participant must complete an evaluation to obtain CE credit
  - Instructions will also be emailed to the program registrant

# *Staying Safe & Secure in an Increasingly Hostile Cyberworld*

# Introduction

**DENNIS JOY**
BS, MS

Director of Information Technology
Forum Extended Care Services

**BRIAN H. KRAMER**
BS, BA, RPh, MBA

President & CIO
Forum Extended Care Services

# Learning objectives

1

Explore data security and ways to mitigate risk in your organization

2

Learn about HIPAA & rules for social media and the internet

3

Understand how to protect your organizations & residents

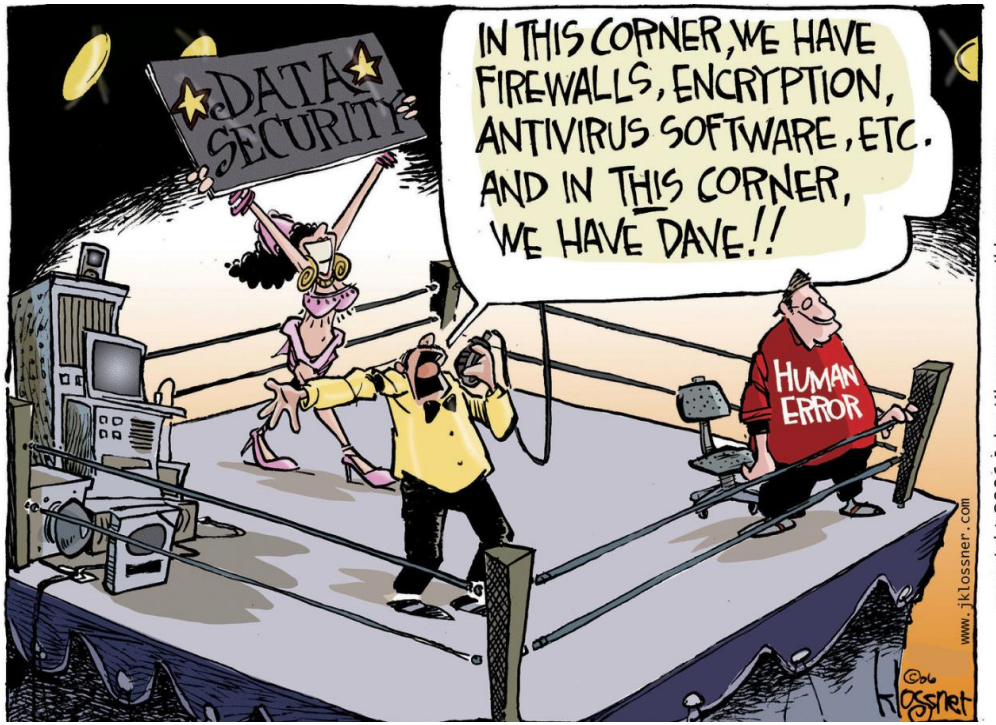
# I have residents/clients/patients to take care of!

# Does IT hate me?

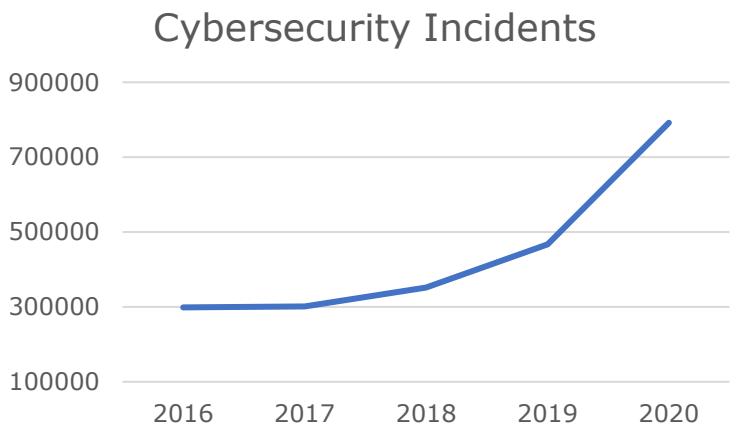
No!

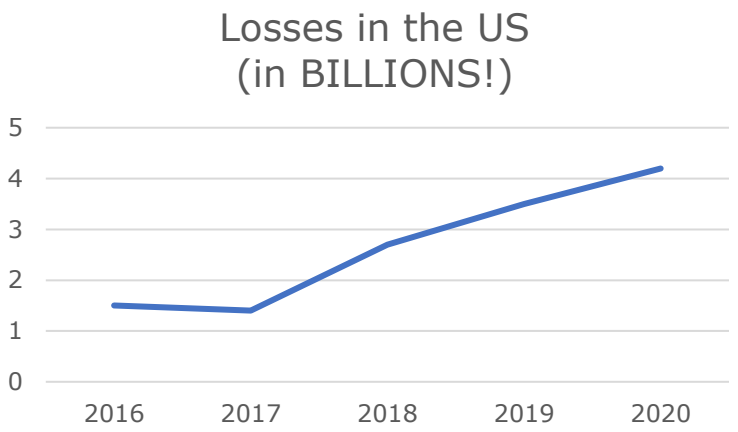
Cybersecurity is a TEAM effort.

We cannot afford to think of it as something for the IT department to handle. Investing in the best security systems won't help if someone leaves the door wide open.



# The threat is real!

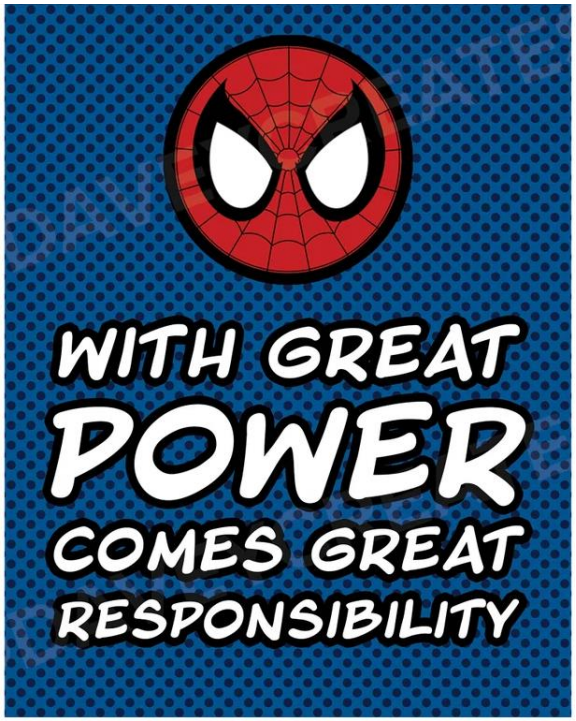


# Fine, but why is it so complicated?

Technology has allowed for increased communication, easier access, and faster processing.

However, each new technology also introduces security and privacy concerns.



# Evolution of technology



Health Insurance Portability and Accountability Act


THE
HITECH
ACT

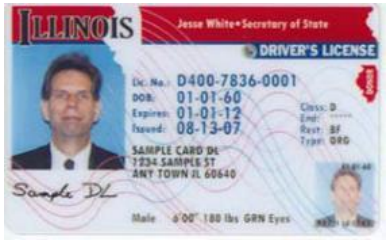
# How do we implement cybersecurity?

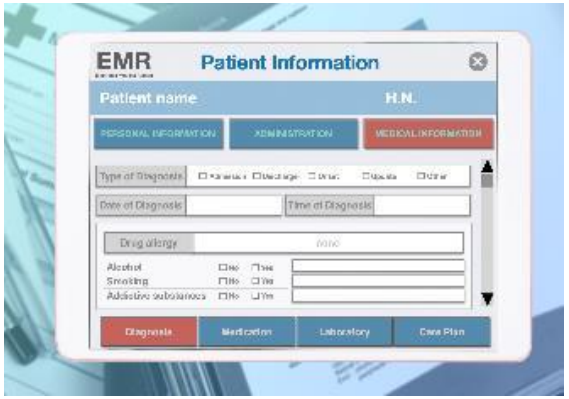
There are several approaches that can be used to mitigate security and privacy concerns in healthcare. We currently use the NIST [National Institute of Standards and Technology] Cybersecurity Framework.

# IDENTIFY

The first step in the NIST Cybersecurity Framework is to identify the data we are obligated to protect.

Once we know WHAT we are protecting, we need to determine WHERE it is created, stored, and transmitted.






# PROTECT

The “CIA Triad” is an important way to understand the different but interconnected security measures we need to take to protect data.

# PROTECT: Common Safeguards

- **Technical**
- Physical
- Administrative

# PROTECT: Common Safeguards

- Technical
- **Physical**
- Administrative

# PROTECT: Common Safeguards

- Technical
- Physical
- **Administrative**

# DETECT

- How will we detect a cybersecurity incident?
- Who's responsible for checking?
- Where is it documented?

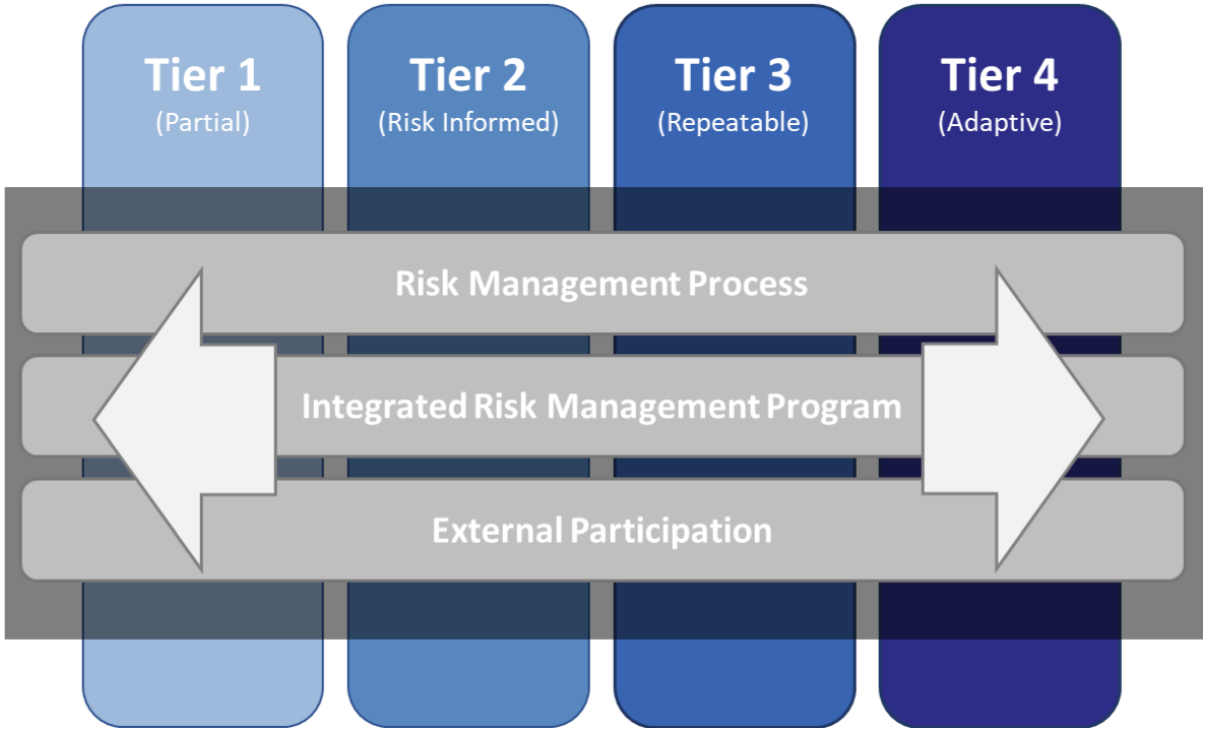
# RESPOND

- If and when an incident happens, what's the plan?
- Are the different responsibilities documented?
- Who's in charge of communicating the response, both internally and externally?

# RECOVER

- Is there a Disaster Recovery & Business Continuity Plan?
  - **Has it been tested in the last year / ever?**
- What's the expected time to recover from backups?
- What's the off-site capability?
- How can we improve?

# Framework Implementation Tiers



# NIST Cybersecurity Framework training

- https://www.nist.gov/cyberframework
- Detailed explanation of framework
- Online learning
- Presentations and other resources
- All FREE!

**Online Learning**

Intro material for new Framework users to implementation guidance for more advanced Framework users.

**Learn More**

# HHS 405(d):
## Aligning Health Care Industry Security Approaches

- https://405d.hhs.gov/protect
- More approachable for non-technical folks
- Also FREE!

# HHS 405(d): Top 5 Threats

- E-mail phishing
- Ransomware
- Loss / Theft of equipment
- Insider, Accidental, or Intentional Data Loss
- Attacks against connected medical devices

# Practical Tips: Passwords

We all have too many passwords!

Best practice is to use a password manager and multi-factor authentication wherever available.


# Practical Tips: Passwords

We all have too many passwords! Best practice is to use a password manager and multi-factor authentication wherever available. If that's not possible, make sure you do the following:

Hard to guess

Don't share

Don't write down

# Practical Tips: Phishing

Email is critical BUT it's also the most likely source for data loss.

Attackers use psychology to tailor their attacks:

- Intimidation
- Impersonation
- Urgency

PREVENT phishing by:

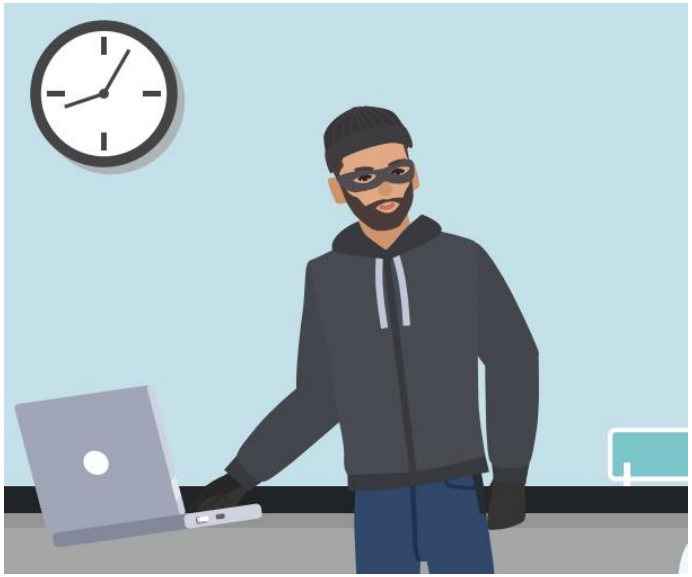
- Limiting social media
- Double-checking links / content / senders
- Using MFA
- Taking it seriously

# Practical Tips: Ransomware

- Phishing is how ransomware attacks frequently begin
- Mitigated by:
  - Routine backups
  - Routine testing of data restoration capability
  - Workstation security

# Practical Tips: Securing Equipment

- Do not leave equipment unattended
- Encrypt all mobile equipment AND require passwords for use
- Notify IT immediately so they can terminate system access



# Practical Tips: Data loss

- Notify IT immediately if you make a mistake
- Report odd behavior by users trying to get access to information they don't need for their roles

# Practical Tips: Connected Medical Devices

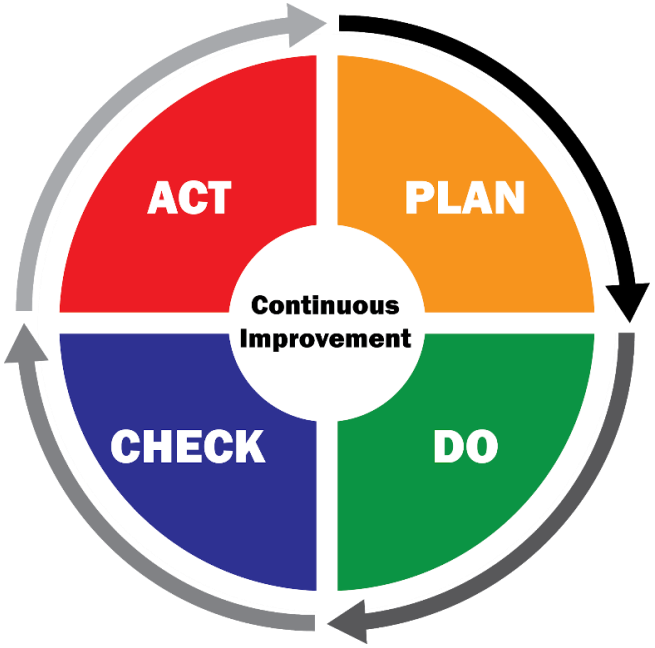
- Notify IT immediately if you notice malfunctions
- IT should limit network access to these devices as much as possible

# A few more things …

- Never pay the ransom
- Get cybersecurity insurance
- Prevent “shadow IT”

# Practical Tips: Continuous Improvement

- One step at a time!
- Document, Document, Document.




# Q & A

# About CE credit

## Administrator credit

This program has been approved for one clock hour of continuing education credit by the National Continuing Education Review Services (NCERS) of the National Association of Long-Term Care Administrator Boards (NAB).

Approval #20230924-1-A87218-DL

## Nursing credit

This program has been approved for one clock hour of continuing education credit by The Illinois Board of Nursing, an approved sponsor of continuing education by the Illinois Department of Professional Regulation.

# Obtaining CE credit

- Complete the evaluation at the conclusion of this program:
  - In your web browser
  - Also emailed immediately following this program
- For those sharing a computer to view the webinar:
  - Submit your sign-in sheet to the email address listed on the form
  - Each participant will then be emailed a link to the evaluation
  - Each person must complete an evaluation to receive CE credit
- Certificates should be **emailed in the next 30 days**

ForumPharmacy.com

## Want more CE after this?

## Look for our upcoming webinars:

**Dec:** *TBD*

**Jan:** *TBD*

**Feb:** *TBD*

**Mar:** *TBD*

# THANK YOU!