NAVIGATING DIGITAL DATA AND MANAGING CYBERSECURITY COMPLIANCE

Jennifer Griveas & Michael Gray
Eliza Jennings Senior Care Network

HCCA Managed Care Compliance Conference
Tuesday, January 30
9:45 - 10:45am

WHO WE ARE

Michael Gray, CISSP, HCISPP, HIT

Mr. Gray is one of fewer than 1,500 dual CISSP/HCISPP certification holders nationwide. Mr. Gray joined Eliza Jennings in 2008 and now serves as Vice President of Information Technology and Compliance Officer. He is responsible for ensuring that the company mission is met using technology, maintaining various compliance requirements, making sure that the department meets and exceeds quality benchmarks and ensuring that the organization can meet future challenges. His major areas of focus are on IT risk management and regulatory compliance. Mr. Gray also leads IT security training.

Jennifer Griveas, Esq., LNHA, CEAL, CEHCH, CHC

Ms. Griveas joined Eliza Jennings in 2011 and serves Vice President & Chief Legal Officer for the organization. She works extensively with the company's board and management on matters of employee relations, as well as health care compliance and security concerns. She also oversees all legal matters for the organization. Prior to joining Eliza Jennings, Ms. Griveas practiced law at Frantz Ward LLP in the firm's labor and employment and litigation groups, where she focused on litigation and employment counseling for clients in numerous industries, including health care and social service providers.

What should scare you?

Gain a better understanding of various threats to data (employee and patient!)

Why should it scare you?

Health care is a prime target for cyber attacks – creating operational AND legal nightmares.

How to train staff and mitigate the risk

Learn about innovative employee training formats to help reduce organizational risk of HIPAA breaches, including crucial role-based training

“You just can’t provide care the same way via telehealth, we’ll always do in-person visits.”

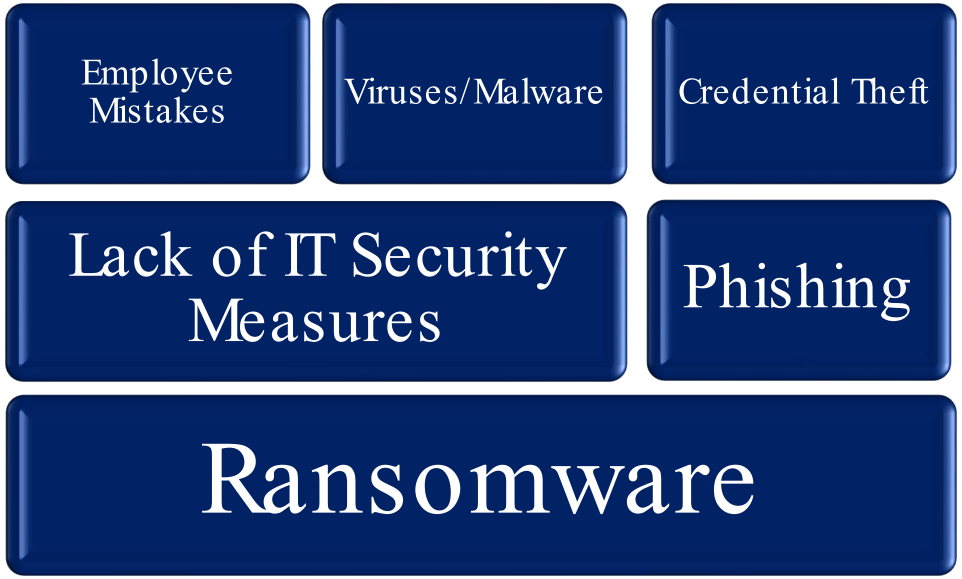
“People can’t work at home in health care!”

“Everybody needs an e-mail address. How else would we communicate?”

“Our people will never give up paper.”

Things we used to say…

We aren’t saying this anymore. What do we need to worry about now that the workforce looks different?



Employee Mistakes

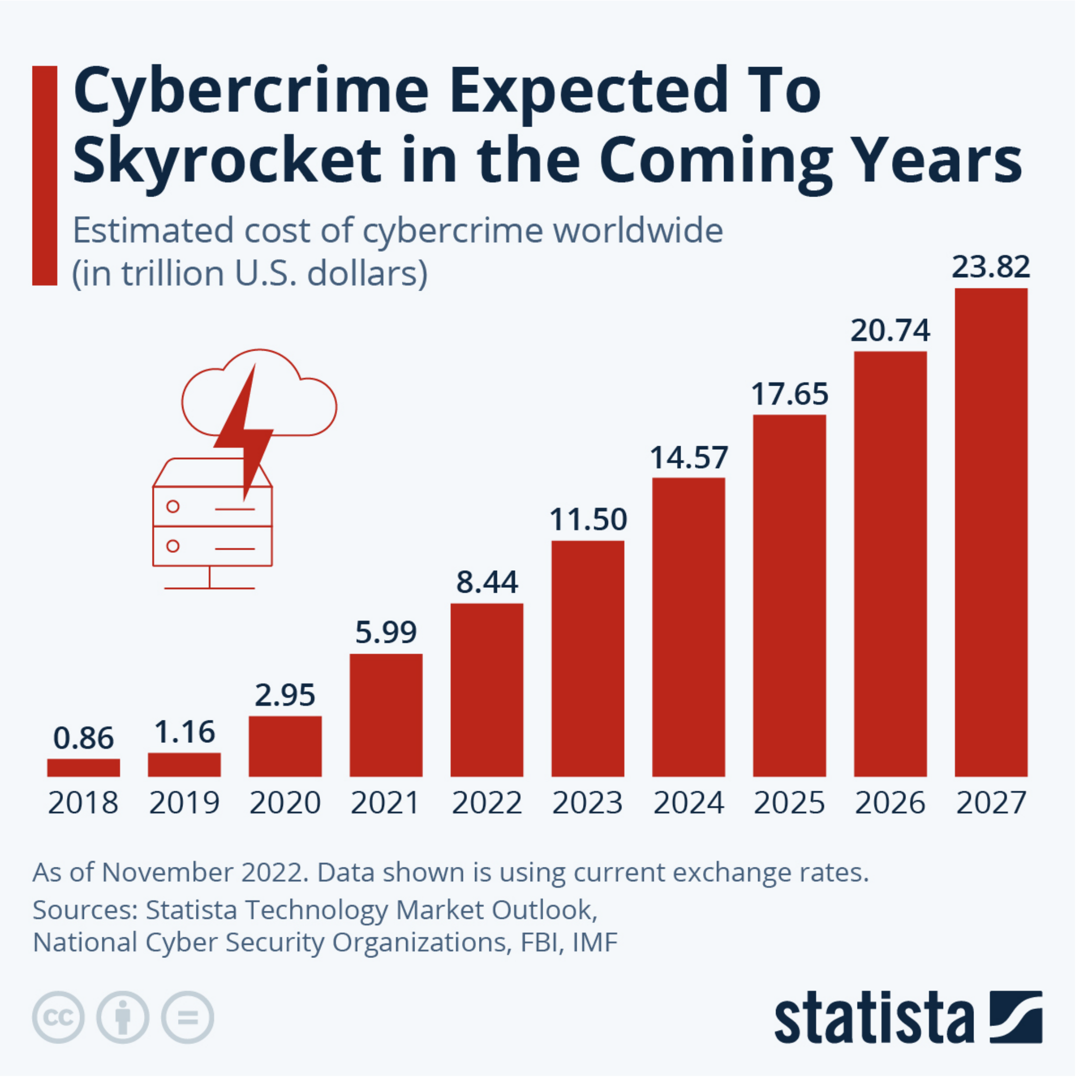
Viruses/Malware

Credential Theft

Lack of IT Security Measures

Phishing

Ransomware



Cybercrime Expected To Skyrocket in the Coming Years

Estimated cost of cybercrime worldwide (in trillion U.S. dollars)

As of November 2022. Data shown is using current exchange rates.

Sources: Statista Technology Market Outlook, National Cyber Security Organizations, FBI, IMF

Cybersecurity threats can impede a healthcare organization’s ability to provide necessary patient care. These threats come from various internal and external sources.

1 Phishing

2 Malware

3 Ransomware

4 Theft of patient data

5 Insider threats

6 Hacked IoT devices

Sources: Center for Internet Security, CSO, Healthcare IT News, TechRepublic

Your employees are the biggest cyber threat whether they know it or not. Your workforce looks different now…so should your training!

A refresher on the law

How do I navigate the MILLIONS of laws, rules, and policies covering health providers, employers, AND data security?

- You need a compliance plan! (Per the ACA, COPs)
  - Training is a vital part of any compliance plan
  - HIPAA is a MAJOR structural component

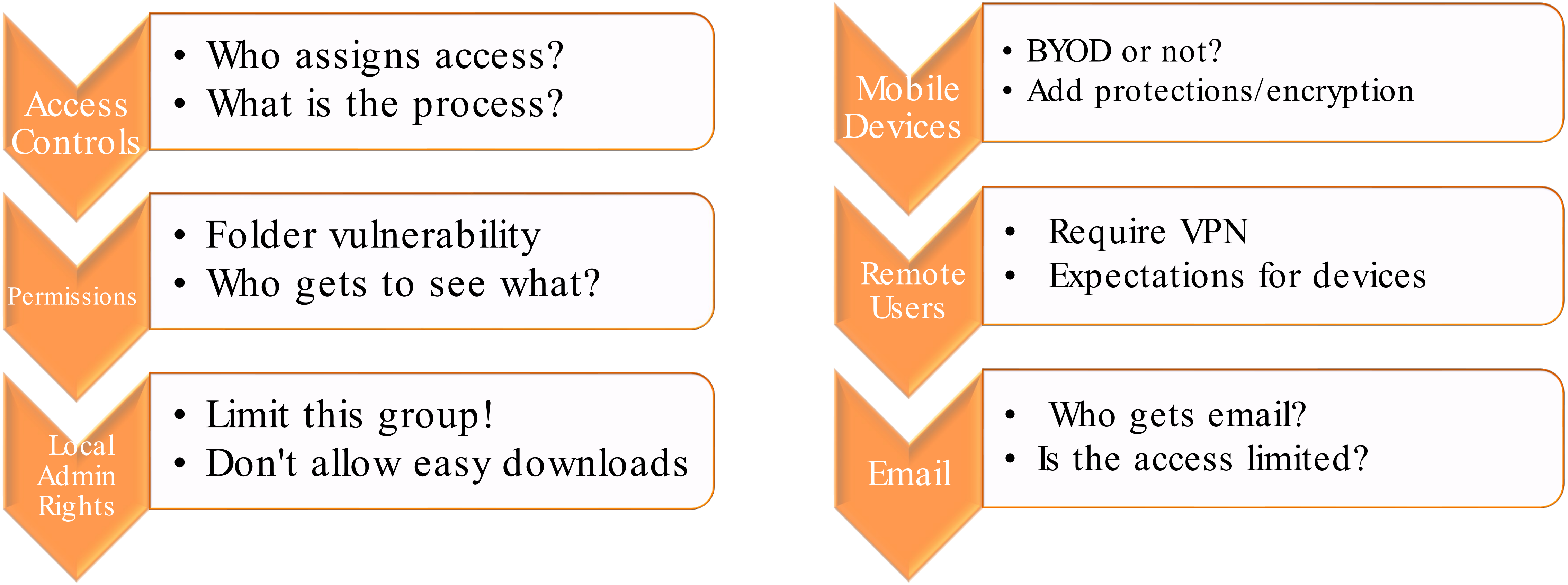
- For Health Care providers, HIPAA is the elephant in the room
  - We get the privacy stuff (mostly...)
  - HIPAA Covered Entities (that's us!) struggle with HIPAA's security rule
  - Do you have a Security Rule Risk Assessment? If so, how dusty is that document?

- States are starting to really care about this data security business!
  - State data protection statutes

  + COPs, Emergency Preparedness, and more!

Before Training: Make Decisions

Strong policies + meaningful training = informed employees and decreased risk



Access Controls

- Who assigns access?
- What is the process?

Permissions

- Folder vulnerability
- Who gets to see what?

Local Admin Rights

- Limit this group!
- Don't allow easy downloads

Mobile Devices

- BYOD or not?
- Add protections/encryption

Remote Users

- Require VPN
- Expectations for devices

Email

- Who gets email?
- Is the access limited?

Universal Training: What Everybody Needs to Know

Threats

- Data theft
- Ransomware
- Lost/stolen device

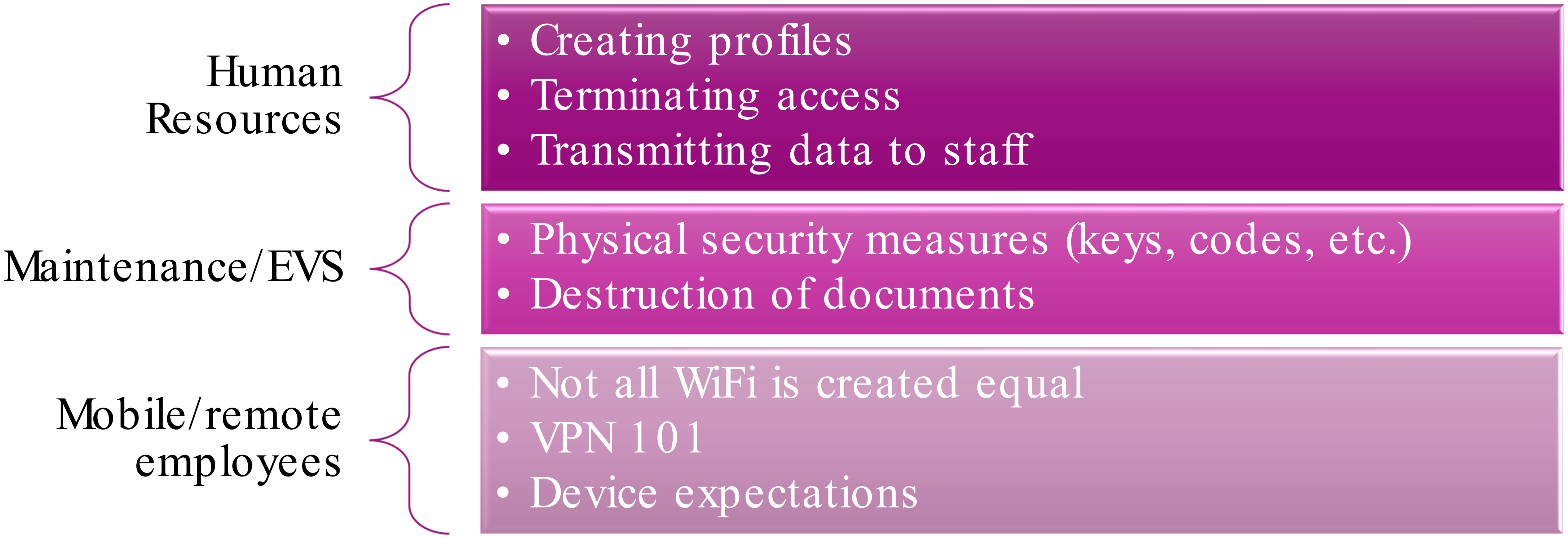
Law/Policy

- HIPAA
  - Privacy
  - Security
  - What is PHI
- Documentation
- Care and use of devices
- Unique credentials
- Passwords

What to Do

- How to dispose of paper, data
- How to communicate within/outside of company
- If device malfunctions
- Device lost/stolen
- 2FA/MFA

Role-based Training: Bite-Sized Info Related to Duties



Human Resources

- Creating profiles
- Terminating access
- Transmitting data to staff

Maintenance/EVS

- Physical security measures (keys, codes, etc.)
- Destruction of documents

Mobile/remote employees

- Not all WiFi is created equal
- VPN 101
- Device expectations

Mobile Device Users: Key information

About the Device

- Do not share
- Encryption features
- Enforce policies/restrictions
- Permission to remove from facility

How to Connect

- Rules on WiFi
- VPN use
- Apps

Mobile/remote employees

- What to do if lost/stolen
- Do I have to deal with this update?
- Device security on the go

Email Users

Email is the biggest target for Ransomware

Know how to spot suspicious emails

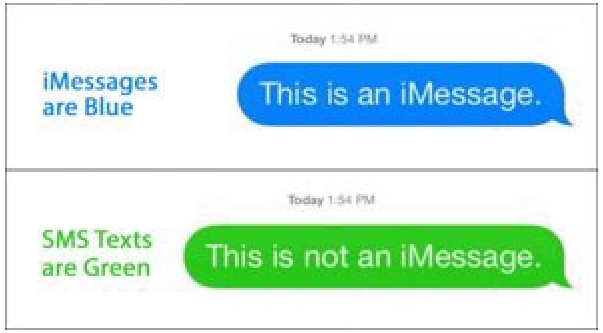
Common email scams

Encryption

Best practices

What to do with suspicious email

Text Communications



Today 1:54 PM

iMessages are Blue

This is an iMessage.

Today 1:54 PM

SMS Texts are Green

This is not an iMessage.

Texts containing PHI can be sent if mechanisms are in place to comply with the technical safeguards of the HIPAA Security Rule

Not all texting is secure!

SMS and some instant messages give no control over final destination

SMS texting lacks encryption, texts may be stored by telecom vendor/ wireless carrier

Texting ePHI should only be via a system with access controls, audit controls, and method of removing messages from a device and archiving them securely

Telehealth and IOT

Telehealth

- Not all are created equal
- Pandemic exceptions have ended
- Understand processes and differences with technology
- Documentation still necessary – what is the process?

Eliza Jennings
choices for aging well

Jennifer Griveas, Esq., LNHA, CEAL, CEHCH, CHC
Vice President and Chief Legal Officer

jgriveas@elizajen.org

Michael Gray, CISSP, HCISPP, HIT
Vice President of Information Technology

mgray@elizajen.org

SCAN ME