



# HIPAA PASS Privacy and Security Solutions

## HIPAA Series: “Securing your New Remote Workforce”

Presented by Susan Clarke

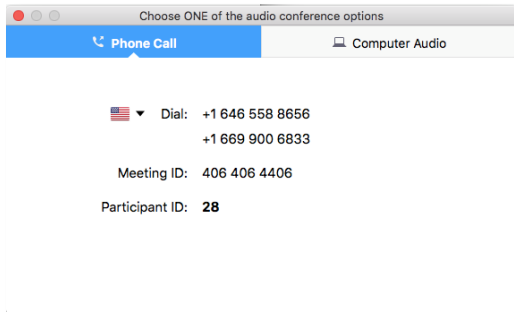
Health Care Information Security and Privacy Practitioner

Thursday, December 17 | 11:00 a.m.



# Zoom tips and tricks!

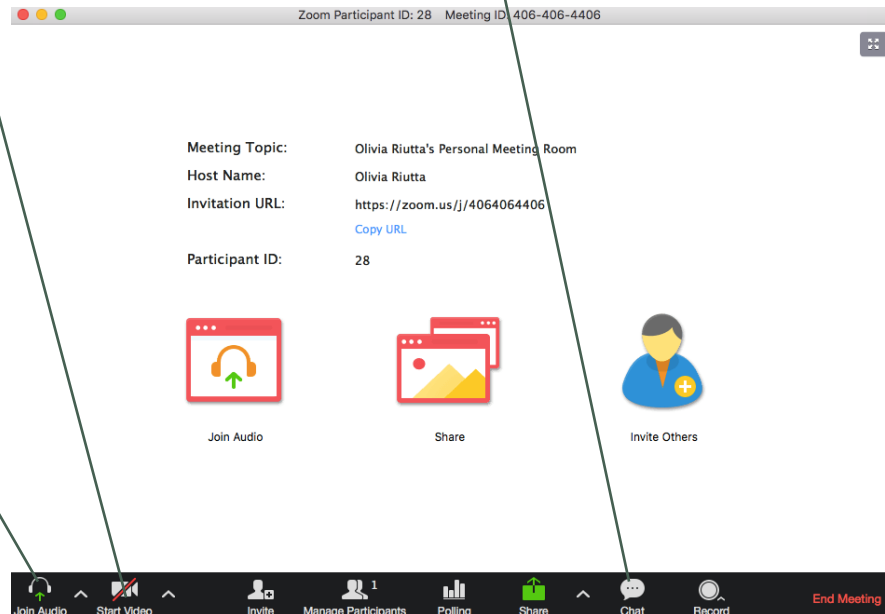
**CHAT:** Please jump in if you have something to share, but we also have this nifty chat function.



**VIDEO:** We want to see you!  
If your camera isn't on, start your video by clicking here.

**AUDIO:** You can use your computer speakers or your phone for audio. The phone is generally better quality. If you click "Join Audio," this "Choose one..." box will pop up. If you dial in, just make sure you include your audio code.

**MUTE/UNMUTE:** \*6 or click the mic on the bottom left of your screen.



**ATTENDANCE:** If there are multiple attendees together on the call, please list the names and your location in the chat box

# Upcoming HCCN Sessions

---

## TELEHEALTH TUESDAY SESSIONS

3<sup>rd</sup> Tuesday of each month at 11:00 a.m.

January 19  
February 16  
March 16  
April 20  
May 18  
June 15  
July 20  
August 17  
September 21

## OTHER HCCN EVENTS

UDS Office Hours with Leslie Southworth

Office Hours from 10:00-11:00 a.m.

December 3, 10, 17  
January 7, 14, 21, 28

**HIPAA Webinar Series with Susan Clarke**

Thursday, March 25 at 11:00 a.m.

Thursday, June 17 at 11:00 a.m.

Thursday, September 16 at 11:00 a.m.

Thursday, December 16 at 11:00 a.m.

## MPCA Events



# Susan Clarke, HCISPP



(ISC)<sup>2</sup> Healthcare Information Security and Privacy Practitioner and Computer Scientist at Mountain-Pacific Quality Health.

Conducts privacy and security risk analysis in addition to HIPAA and 42 CFR, Part 2 training.

20 years' experience in health care operations.

10 years' design and coding EHR software including HL7 Healthcare application development.

Served on IT security, disaster recovery and joint commission steering committee at Mayo Clinic-affiliated health care system.

# Legal Disclaimer

*The presenter is not an attorney and the information provided is the presenter's opinion and should not be taken as legal advice. The information is presented for informational purposes only.*

*Compliance with regulations can involve legal subject matter with serious consequences. The information contained in the webinar and related materials (including but not limited to recordings, handouts and presentation documents) is not intended to constitute legal advice or the rendering of legal, consulting or other professional services of any kind. Users of the webinar and webinar materials should not in any manner rely upon or construe the information as legal or other professional advice. Users should seek the services of a competent legal or other professional before acting or failing to act, based upon the information contained in the webinar to ascertain what may be best for the users' needs.*





# Acronyms

**BA:** Business Associate

**BAA:** Business Associate Agreement

**CE:** Covered Entity

**CEHRT:** Certified Electronic Health Record Technology

**CMS:** Centers for Medicare & Medicaid Services

**EHR:** Electronic Health Record

**ePHI:** Electronic Protected Health Information

**HHS:** Department of Health and Human Services

**HIPAA:** Health Insurance Portability and Accountability Act

**HIT:** Health Information Technology

**IT:** Information Technology

**NIST:** National Institute of Standards and Technology

**OCR:** Office for Civil Rights

**PHI:** Protected Health Information

**QSO:** Qualified Service Organization

**SP:** Special Publication

**SRA:** Security Risk Analysis

# HIPAA Notice of Proposed Rulemaking

On December 10, 2020, Health and Human Services (HHS) issued a notice to modify HIPAA Privacy Rule as part of the Regulatory Sprint to Coordinated Care,

The proposed changes are regarding:

1. Strengthened access for patients to their records (including electronic).
2. Improved information sharing policies regarding care coordination and case management.
3. Improved policies to facilitate family and caregiver involvement for health emergencies or crises.
4. Enhanced flexibility for disclosure in public health emergencies.
5. Proposed reduction of admin burdens for health centers, specifically Notices of Privacy Practices

<https://www.hhs.gov/sites/default/files/hhs-ocr-hipaa-nprm.pdf>

# Learning Objectives



Remote network management from home



Reinventing the way we work—distributed, secure, flexible



The last byte on compliance





## Remote Network Management from Home

# Remote Access Overload



Pushed beyond limits during COVID-19

# Remote Workforce



Health care IT departments are facing a great, once-in-a-lifetime challenge.

*Almost overnight, routine operations and services have become radically changed — possibly forever.*

# Dispersed Workforce

## Challenges

We will discuss tools and practices to



stay on top of routine network operations,

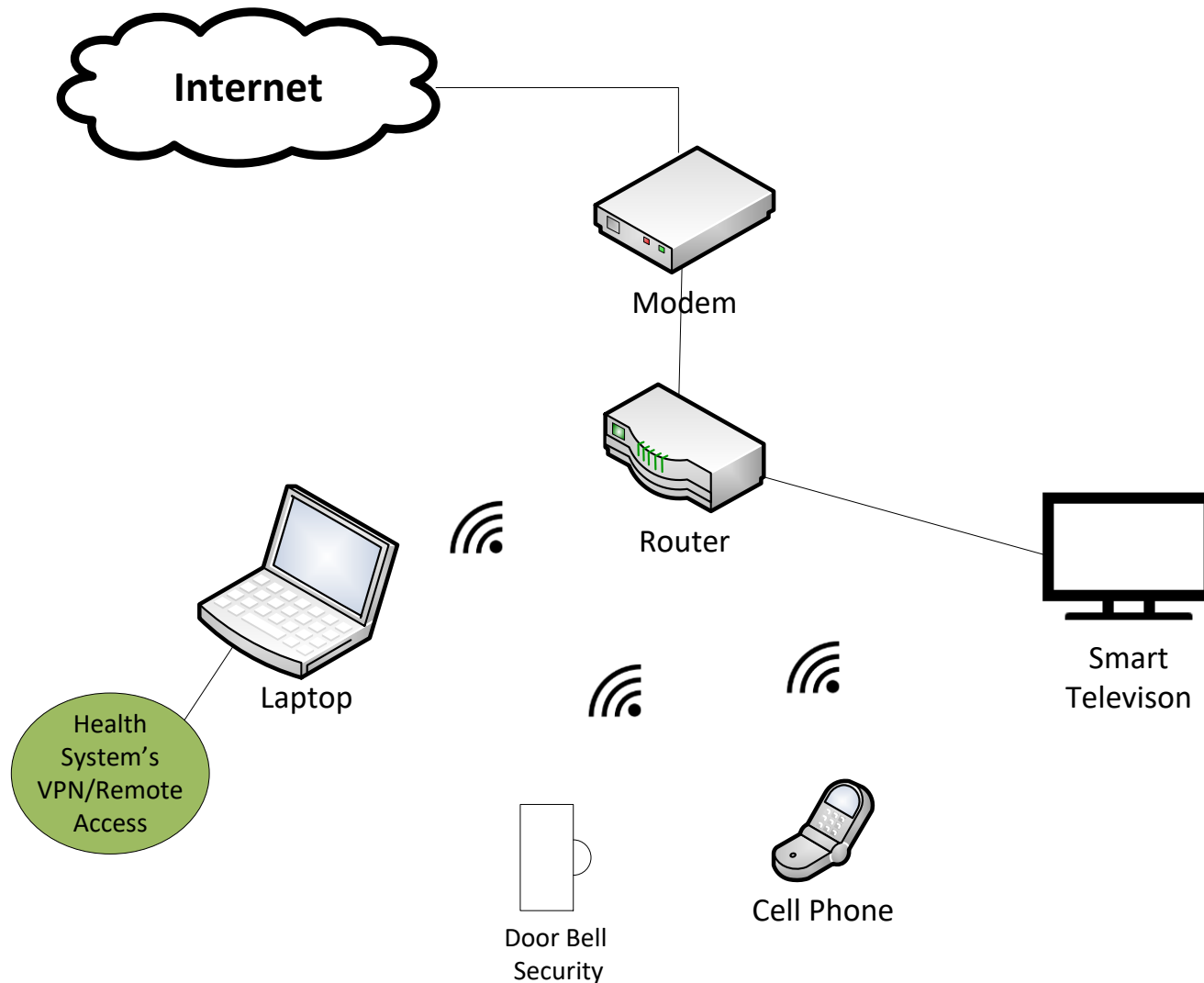


monitor performance,



resolve issues while keeping current and planned projects moving forward.

# Example Home Network



# Legacy VPNs

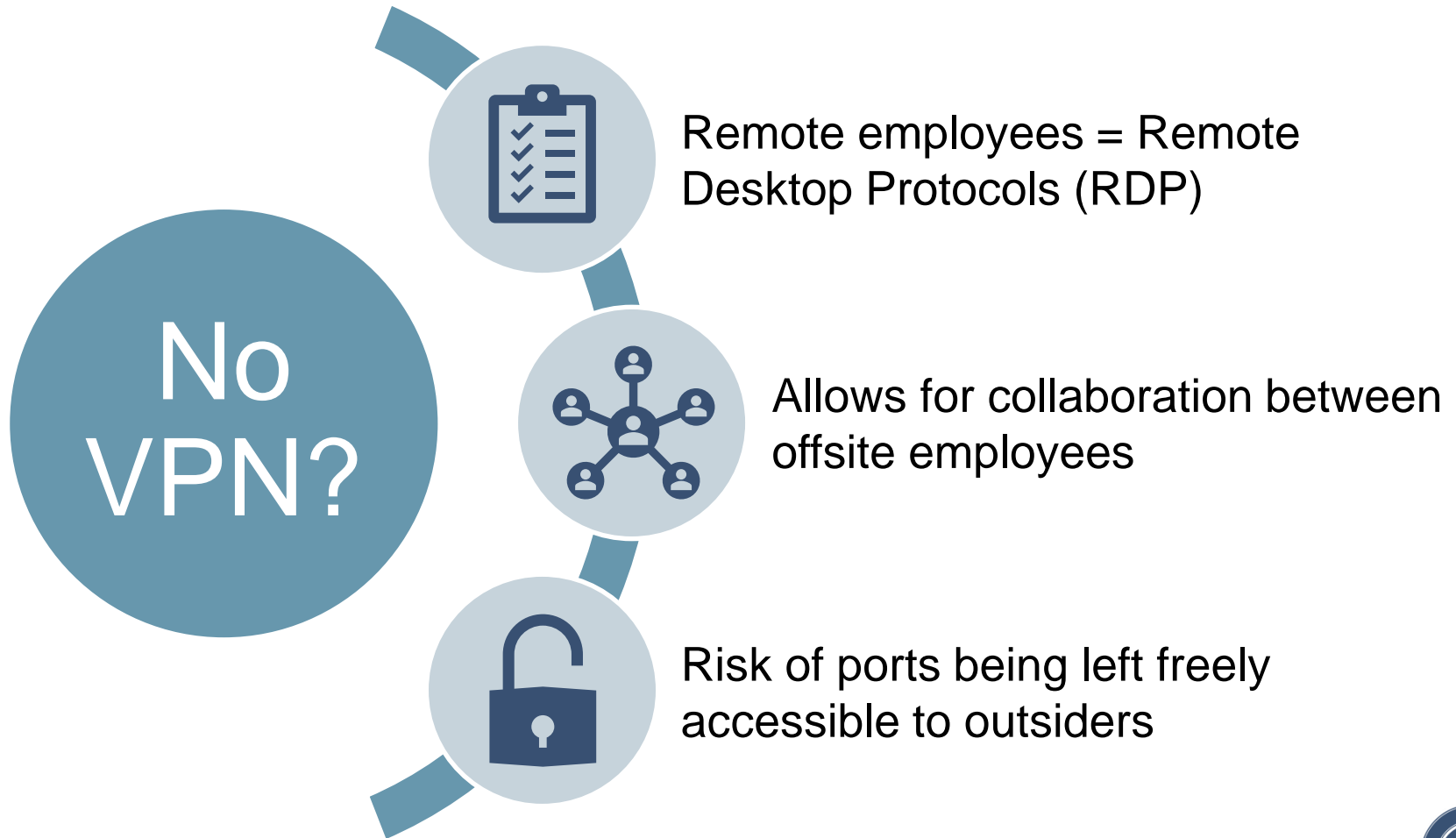
- Beginning to show performance and security cracks
- Not built to support large numbers of users

So organizations should...

- Evaluate connectivity options
- View COVID-19 as opportunity to modernize network infrastructure



# Remote Workforce Workarounds



# No Big Easy Button

## Software-Defined Networking in Wide Area Network (SD-WAN)

Designed to fully support tools and applications hosted in on-premises data centers or in public or private clouds

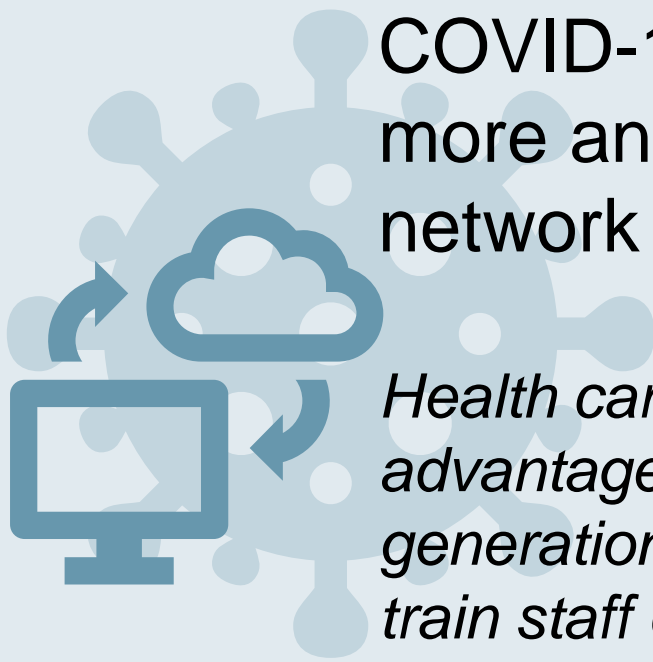
## Secure Access Service Edge (SASE)

- Alternative to traditional SD-WAN technology
- Offers more benefits



Important: Understand your network needs.

# Embracing Automation



COVID-19 exposed the need for more and enhanced autonomous network operations.

*Health care IT should consider taking advantage of capabilities provided by a new generation of network automation tools and train staff on key technologies.*



Reinventing the Way We Work—  
Distributed, Secure, Flexible

# Understanding Risk



Cyber risk increases with expanding cyber attack surface.



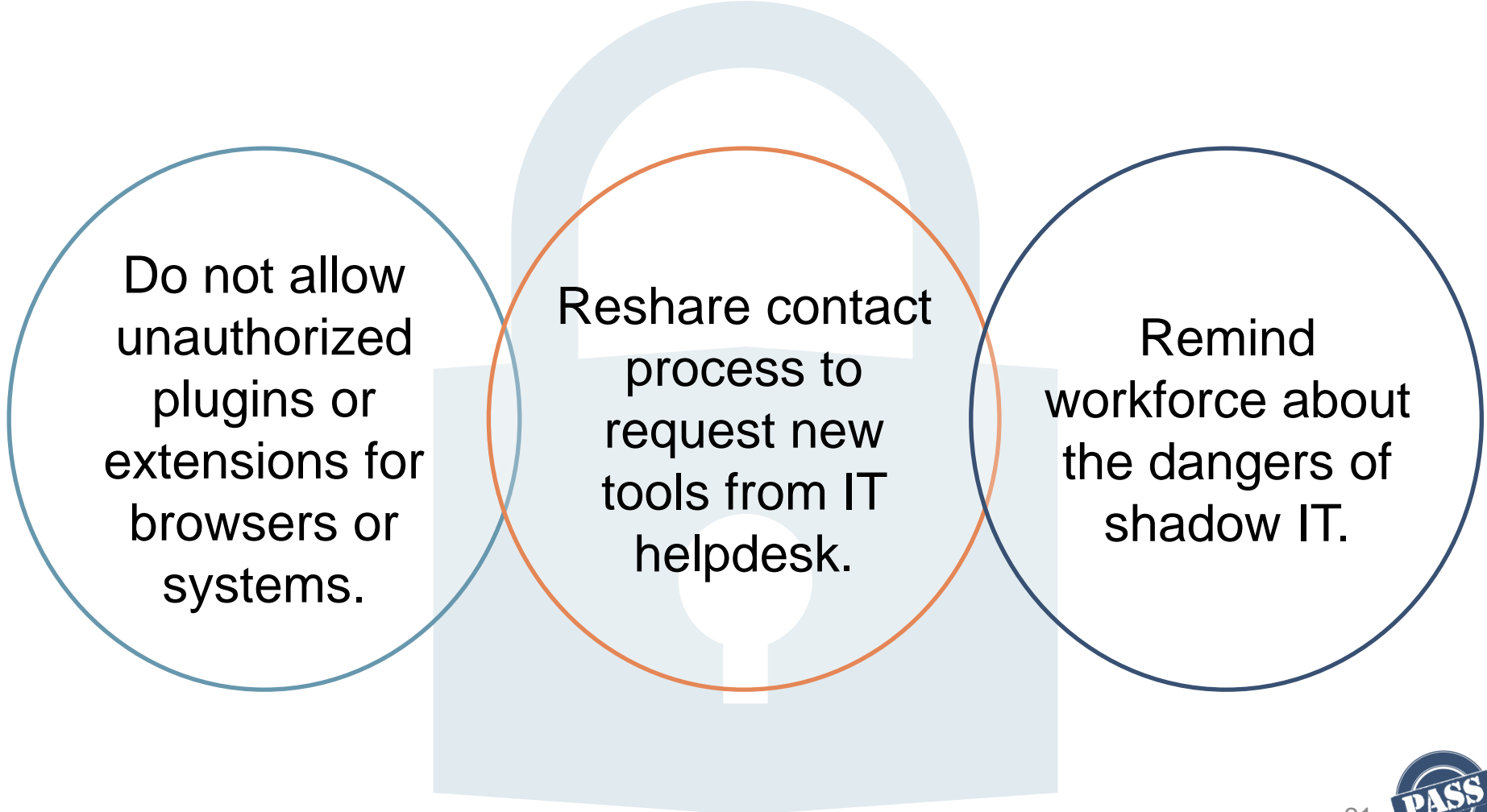
Security perimeter has been decentralized.

# Shadow IT

- 1 Need for a tool not currently provided
- 2 Desire to improve ease and efficiency of work
- 3 Perceived need to circumvent existing security protocols to complete work tasks



# Security Reminders



Do not allow unauthorized plugins or extensions for browsers or systems.

Reshare contact process to request new tools from IT helpdesk.

Remind workforce about the dangers of shadow IT.

# Be Progressive

*What might make  
your work product  
better?*

*What might make  
your work product  
stronger?*

*What might make  
your work product  
faster?*

Employee surveys help adapt approved corporate technology stacks and avoids unwelcomed surprises.

# Home Network Vulnerabilities

Risk factors for employees using their existing WiFi to access corporate networks and to retrieve and save sensitive information include:

- ❑ Routers with outdated software, factory password unchanged
- ❑ Internet of things (IoT) devices left on public default settings
- ❑ Lack of employee training regarding cybersecurity best practices

# Phishing Awareness Programs



Cyber threat campaigns are taking advantage of rapid change in employee circumstances (transition to remote working).



# Guidance for Employees



Be aware of COVID-19 phishing and malware.



Be aware of video conferencing security and privacy issues.



Only use approved devices for work.



Keep laptop and software up-to-date.



Check WiFi and VPN connection.

# Two/Multi Factor Authentication

Electronic authentication method in which user is granted access after successfully presenting two or more pieces of evidence of authentication

- 1) Something you **have** (code on a cell phone)
- 2) Something you **know** (password)
- 3) Something you **are** (fingerprint)

Note: in some cases, location and network indicators are also used as additional authentication factors.





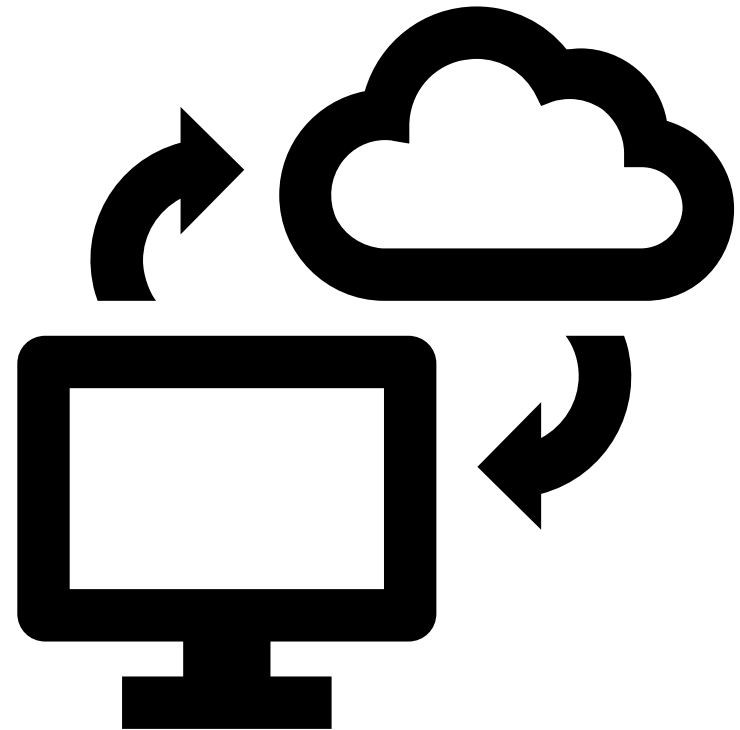


# The Last Byte on Compliance



# Reduce Risk—Backup!

Today, building a bullet proof backup strategy is a must have.



# Business Continuity Plan (BCP)

Review your BCP.

Consider:

- Remote workers
- Reduced operating level
- Essential personnel

Make sure you can operate in various situations.

Determine what you would do should a cyber incident occur.



## Important Section: Contact List

1. Test in tabletop exercise (TTX), even if a small group of people.
2. What you are going to do and how will people stay connected to keep operations running?

# Compliance Concerns

In a perfect post-COVID world, compliance becomes a by-product of a well run and finely tuned security program. However, in times of uncertainty, security controls may need to be partially relaxed.

- 1** *Trade-offs need to be carefully considered and documented and may be appropriate, given the current situation.*
- 2** *Focus on areas where risks cut across the compliance. Make sure you are expressing those to your leadership.*



Please let me know how I can help.

**For assistance, please contact:**

Susan Clarke

[sclarke@mpqhf.org](mailto:sclarke@mpqhf.org) | (307) 248-8179

**Thanks for your  
valuable time today!**

