# *Telehealth Tuesday: Privacy and Security with Telehealth with Susan Clarke*

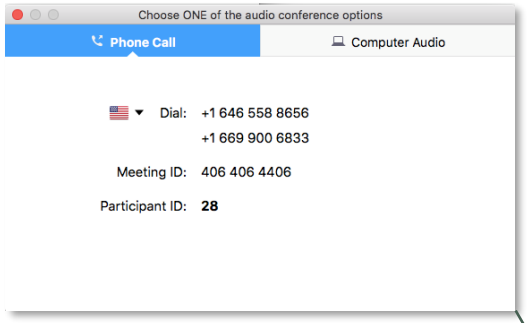
AUGUST 25TH, 2020

# Zoom tips and tricks!

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

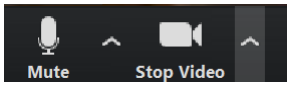
**ATTENDANCE**: If there are multiple attendees together on the call, please list the names and your location in the chat box

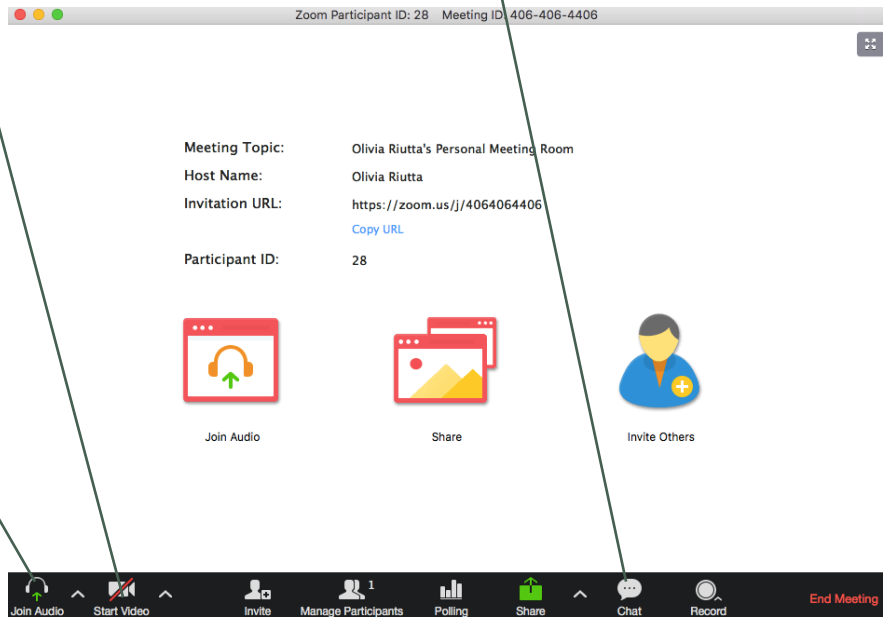
**VIDEO**: We want to see you!
If your camera isn't on, start your video by clicking here.




**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.



# Agenda

- Upcoming Events
- Privacy and Security with Telehealth
- Q&A and Peer Discussion

# Upcoming HCCN Sessions

## TELEHEALTH TUESDAY SESSIONS

**3rd Tuesday of each month at 11:00 a.m.**

September 15

October 20

November 17

December 15

## OTHER HCCN EVENTS

**HIPAA Series: Save the Dates**

The Path to 42 CFR, Part 2, Past, Present and Future"

Thursday, September 24 at 11:00 a.m.

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

azara healthcare 2020 VIRTUAL USER CONFERENCE

September 22-24

MONTANA HEALTHCARE CONFERENCE 2020

2020 Montana Healthcare Conference

October 5 – 9, 2020

HCCN Health Center Controlled Network

MPCA Events

MPCA

# Susan Clarke, HCISPP

- (ISC)$^2$ 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 CRF, 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

**SP:** Special Publication

**SRA:** Security Risk Analysis

# Learning Objectives

Overview of telehealth and HIPAA privacy and security

Relaxing of HIPAA for telehealth during COVID-19

Cybersecurity for your remote workforce

# Telehealth and Security

# The Golden Rule

People and Safety come first.

Leadership buy-in is critically important.

Everyone is responsible for security.

Training is essential.

Policy is the key to almost everything.

# Telehealth Visit Quick Start List

**Choose platform for visits**

- Security
- Practice considerations
- Patient considerations

**Develop priority patient list**

- Patient interest and ability
- Determine Patients at higher risk

**Conduct visit**

- Engage patient
- Schedule visit
- Privacy concerns
- Technology

**Document visit**

- EHR processes
- Pertinent legal considerations

**Bill/reimbursement for visit**

- Medicare
- State Medicaid
- Commercial

# HIPAA and Telehealth

Privacy, security, and confidentiality issues must be addressed in telemedicine the same as in conventional medical practices.

Telemedicine applies to both originating and distant sites which increases the frequency that PHI is available electronically.

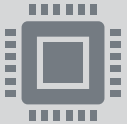
Technical safeguards like encryption provide safe harbor. Make sure data transmission is encrypted.

No control over vendors actions or operations, clearly state in Business Associate agreements. (**Important: the vendor must be willing to sign a BAA.**)

# HIPAA and Telehealth

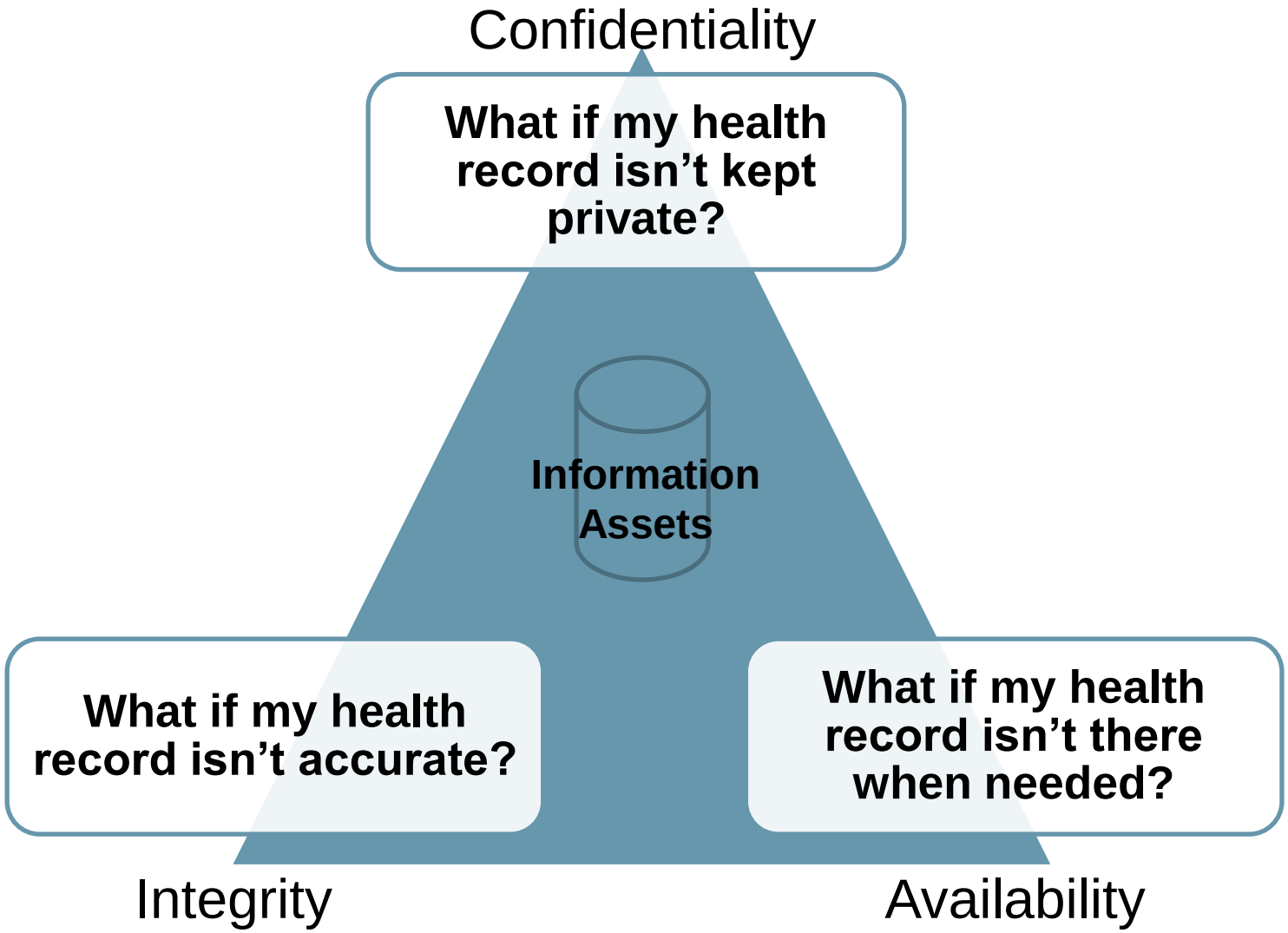
Storage considerations for electronic files, images, etc. EHR vendors starting to store telehealth visits.

Technology used for telehealth needs to ensure high-level of security safeguards and controls.



Understand how and what PHI is being collected and stored.

# IT Security and CIA Triad



# Business Associate

- ✓ Telehealth can have a greater number of platforms, role of telehealth company (BA) in data storage, reporting, billing.
- ✓ BAs must comply with the technical, administrative, and physical safeguard requirements under the Security Rule; liable for Security Rule violations.
- ✓ Technical vendors who can access PHI and work on behalf of provider is a business associate and need a business associate agreement.
- ✓ BA definition expressly includes Health Information Organizations, E-prescribing Gateways and personal health record (PHR) vendors that provide services to covered entities.

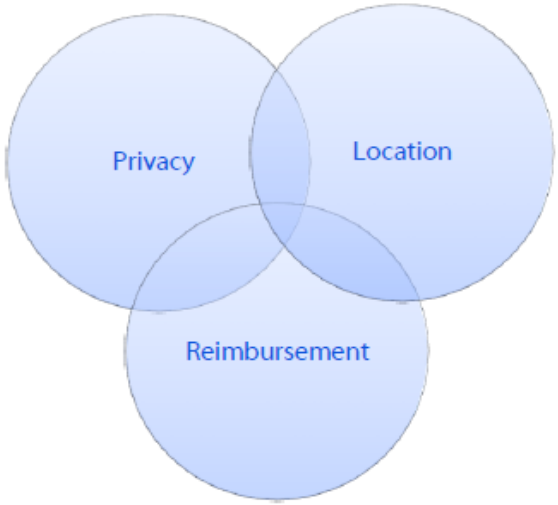
# Telehealth Privacy Considerations

- Consider what type of informed consent from patient before telehealth is used. Explain the purpose, risks, benefits, alternatives.
- State laws vary, if multiple states use strictest to standardize processes.
- There must be a private and uninterrupted space in which the equipment is kept where the client/patient will consult with the provider.
- Providers and patients using televideo equipment often speak louder than normal.
- HIPAA laws that govern use, disclosure and breach must be followed faithfully.
- There should be a door that closes and is able to be locked when room is not is use.
- A telephone is needed as backup in case the televideo connection drops.

# Telehealth during COVID-19

# Recent Legislative and Policy Changes Affect Telehealth Utilization

- HIPAA Flexibility to include new technology platforms.
- Federally qualified health centers (FQHCs) and rural health centers can serve as eligible sites of care for telehealth services during the COVID-19 response.
- Waiver allowing healthcare providers to use telehealth and wherever the patient is located.
- Providers may see both new and established patients.
- Out-of-state practitioners permitted to provide telehealth services in another state.



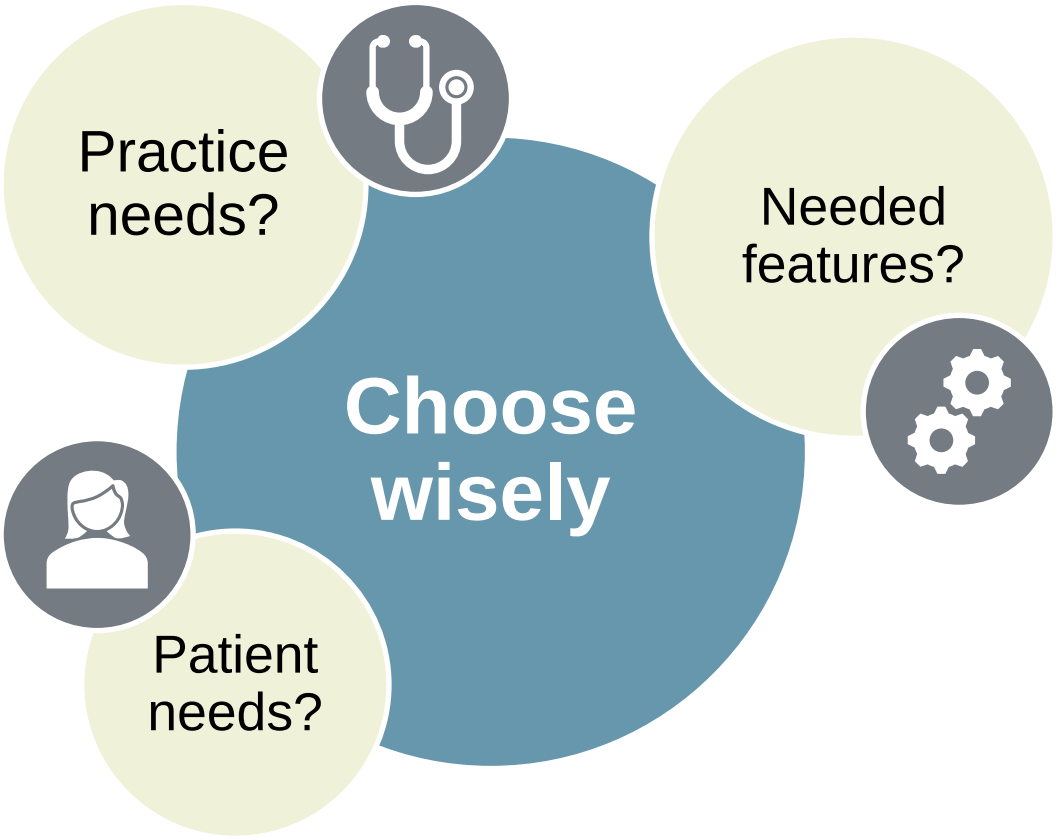

https://telehealth.hhs.gov/providers/policy-changes-during-the-covid-19-public-health-emergency/

# Relaxing of HIPAA to Promote Telehealth Visits during COVID-19

HHS Office of Civil Rights (OCR) will exercise enforcement discretion and waive penalties for HIPAA violations against health care providers who serve patients in good faith through everyday communications technologies (e.g., FaceTime, Skype).

https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html

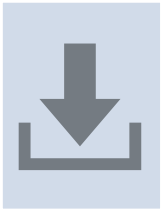
# Choosing Telehealth Software



# Choosing Telehealth Platform

Work on multiple devices

Work over cellular (mobile) and WiFi

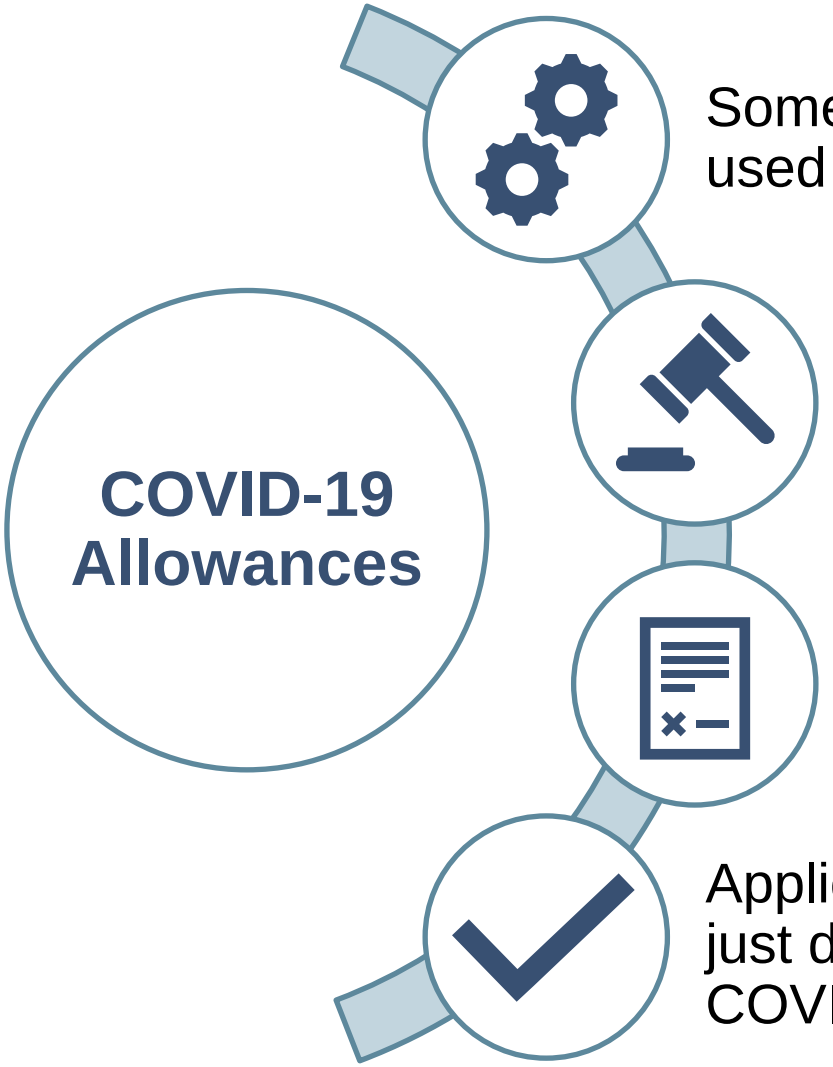


Easy to install

Easy to open

Easy to use

# HIPAA Standing Down for Telehealth




Some technologies and how they are used may not fully comply

OCR will exercise enforcement discretion/not impose penalties for noncompliance (good faith provision)

OCR will not impose penalties against covered health care providers for lack of business associate agreement with vendors

Applies to any telehealth service, not just diagnosis/ treatment related to COVID-19

# Technology

## Acceptable Non-Public Facing Applications

- Apple FaceTime
- Facebook Messenger video chat
- Google Hangouts video
- Skype

Notify patients of potential privacy risks

Enable all available encryption and privacy modes

# Choosing a Platform: Patient Friendly*

## Today's Most Commonly Used Communications during COVID-19

| Vendor | Product | Platform | Encryption/ Authentication | Security Considerations | Collect to Connect |
|---|---|---|---|---|---|
| Apple | FaceTime | Not recommended outside Apple iOS | AES-256-bit, End-to-end | Calls not stored on Apple's servers; iCloud Backup can be turned off | Phone and email or Apple ID |
| Microsoft | Skype | Android, Apple, Windows | AES-256-bit, End-to-end | Data routed through Microsoft; for end-to-end must use Private Conversation | Phone and email or Skype ID |
| Microsoft | Teams | Only works within your Office 365 environment; may not be viable solution | AES-256-bit | Data resides in Office 365; subject to security controls, retention and ediscovery | User ID only if assigned through work |
| Facebook | WhatsApp | Android, Apple, Windows | AES-256-bit, End-to-end | Facebook no access to contacts or conversations | Phone and email or username |
| Facebook | Messenger | Android, Apple, Windows | AES-256-bit, Not encrypted by default | Facebook no access to contacts or conversations; for end-to-end, must use Secret Conversation | Phone and email or username |
| Google | Google Hangouts | Android, Apple, Windows | AES-256-bit & SHA-1 | Some data resides in Google | Phone and email |

http://www.mpqhf.org/corporate/wp-content/uploads/2020/04/Telehealth-Patient-Preference-Vendor-Comparison_508.pdf

# Security Recommendations

| | |
|---|---|
| Set up | Set up service-specific accounts as needed |
| Create | Create better separation for post-COVID-19 discontinuation of these temporary telehealth services |
| Enable | Enable two-factor authentication |
| Find out | Find out if and where any data from the telehealth visit is stored |
| Maintain | Maintain documentation, communication, and confidentiality |
| Manage | Manage patient expectations |

# Common Pitfalls

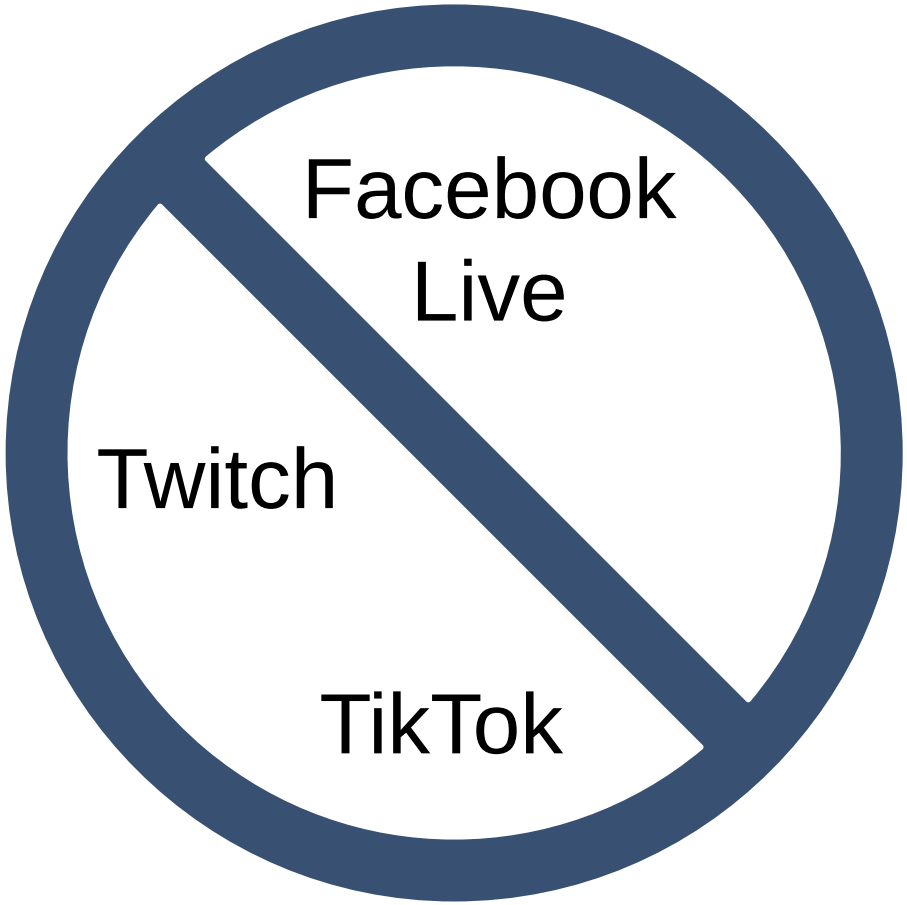
Avoid conducting these telehealth sessions from the clinician's personal accounts

Avoid conducting telehealth visits or patient communication in public

Avoid using video conferencing technology that does not have a unique URL for each session

# Technology

## DO NOT USE PUBLIC-FACING APPLICATIONS



# Potential Telehealth Limitations & Considerations

- Situations in which in-person visits are more appropriate
- Privacy limitations
- Limited access to technological devices (e.g., smartphone, tablet, computer) needed for a telehealth visit or connectivity issues
- Level of comfort with technology for healthcare personnel and patients
- Cultural acceptance of conducting virtual visits

# The New Remote Workforce

# Is Your Remote Workforce Prepared?

## Does your organization have:

- Good data backups?
- Layered security aka defense in depth?
- A strong emergency preparedness program including downtime procedures?
- Investment in training your employees?
- Cyber insurance?

Security systems need to win every time.
Hackers only have to win once.

# Security for Remote Workers

Risk of using personal email on corporate computers

Email security

Security for new remote workers due to COVID-19

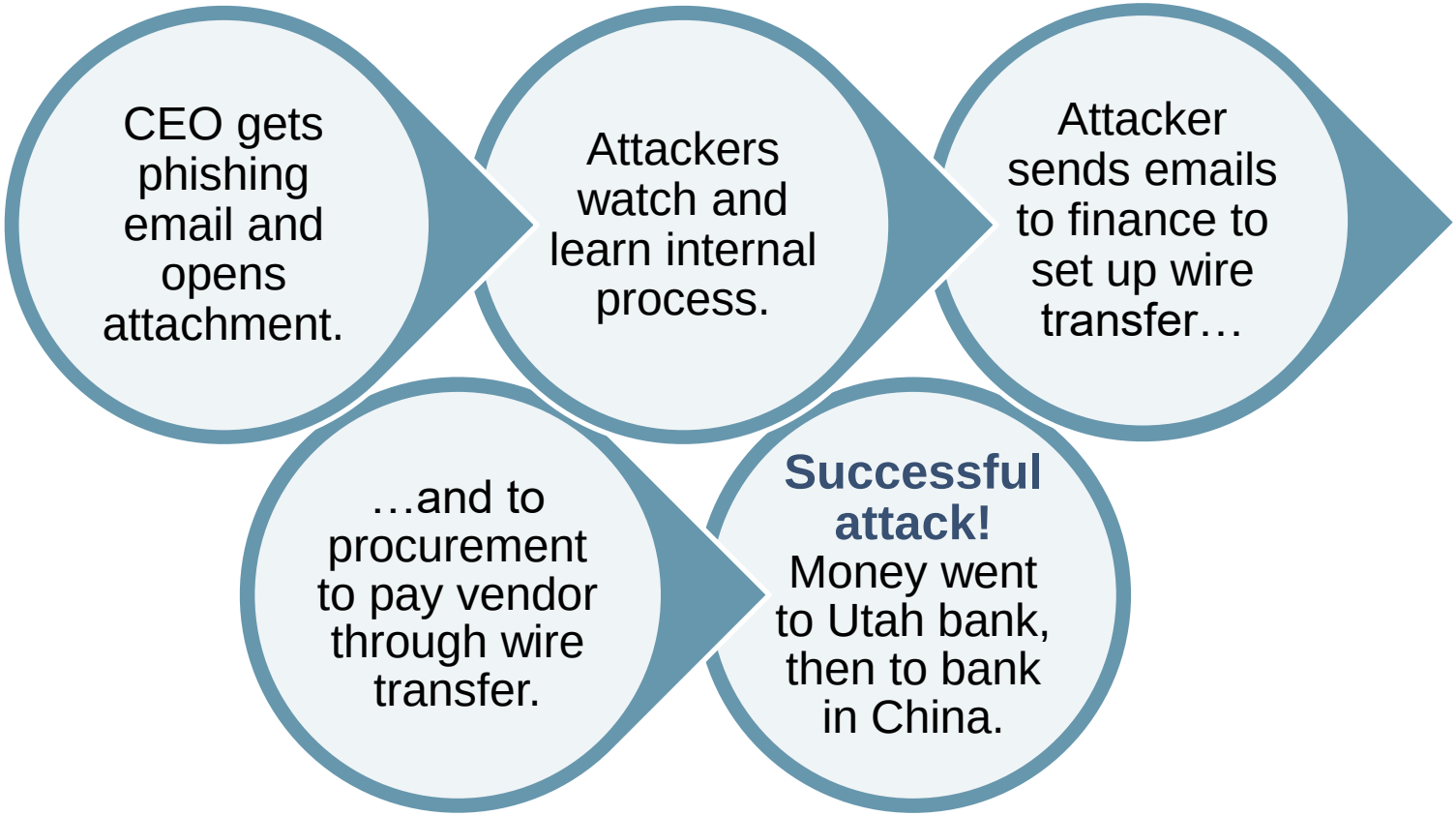
Careful of stress or panic-led disclosures during COVID-19

# Signs of Malicious Email

- To/from/received/reply unconnected
- URLs branding slightly off
- Disconnected/bogus URLs
- Unexpected file attachments
- Internet mail extension type mismatches
- Unexpected requests for actions
- Stressor claims, sense of urgency

# Business Email Compromise Attacks

## Social Engineering




***Empower and train employees to protect your network!***


**ITL BULLETIN MARCH 2020**

# Security for Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Solutions

Karen Scarfone[1], Jeffrey Greene, and Murugiah Souppaya
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2020-03.pdf

# Information Technology Laboratory (ITL) Bulletin Security Measures

| 01 | 02 | 03 | 04 | 05 |
| --- | --- | --- | --- | --- |
| Developing and enforcing a telework security policy, such as having tiered levels of remote access | Requiring multi-factor authentication for enterprise access | Using validated encryption technologies to protect communications and data stored on the client devices | Ensuring that remote access servers are secured effectively and kept fully patched | Securing all types of telework client devices—including desktop and laptop computers, smartphones, and tablets—against common threats |

# How to support a Culture of Compliance

MUST HAVE ENGAGED AND SUPPORTIVE LEADERSHIP.

POLICY AND PROCEDURES ARE STATEMENT THAT YOU ASSERT YOUR INTENT TO COMPLY WITH REGULATIONS. IMPORTANT--YOU MUST FOLLOW.

TRAINING--MAKE SURE YOUR EMPLOYEES ARE YOUR BIGGEST ASSET NOT YOUR BIGGEST LIABILITY.

# Telehealth Resource Material

https://www.telehealthresourcecenter.org/resources/

https://www.cchpca.org/resources/covid-19-telehealth-coverage-policies

to educate our patients on how to connect to telehealth
https://www.avancecare.com/covid-19/

AMA Telehealth Quick Guide: https://www.ama-assn.org/practice-management/digital/ama-telehealth-quick-guide

AMA Digital Health Implementation Telehealth Playbook: https://www.ama-assn.org/amaone/ama-digital-health-implementation-playbook

Link to a reimbursement guide that reviews all of the requirements and options to bill for virtual care.
https://education.hccinstitute.org/Public/Catalog/Details.aspx?id=pyByVKg7JGDSk5TYPpUdsg%3d%3d


**Please let me know how I can help.**

**For assistance, please contact:**

Susan Clarke
sclarke@mpqhf.org | (307) 248-8179

# Thanks for your valuable time today!

# Questions?

Toni Wood, CPHIMS

Clinical Informatics Manager

twood@mtpca.org

(406) 438-1575