




Q & A

HIPAA DISCLOSURES

TELEHEALTH USE

CYBER THREATS

1



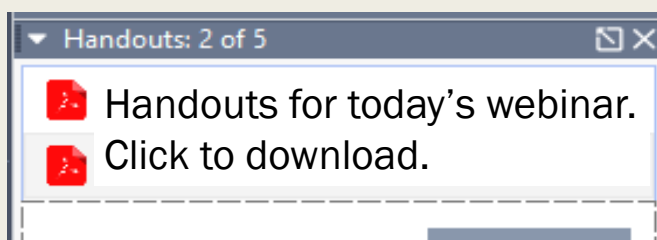
Disclaimer

- Abby Mitchell CHPC, CHC, HCISPP, CRISC is an employee of Total Medical Compliance.
- She serves on the board of directors for the Charlotte, NC chapter of the Information Systems Security Association (ISSA).
- No commercial support has been provided for this activity. Any reference to a commercial product is for example purposes only and does not reflect endorsement.

2

Good to Know

- Continuing education documents only for the live webinar will be provided by THURSDAY, April 16 2020.
- The webinar is being recorded and will be on the [TMC COVID - 19 Resource Page](#)
- Handouts are located on the right side of your screen



- Q and A will be held during the last 10 minutes of the webinar

3

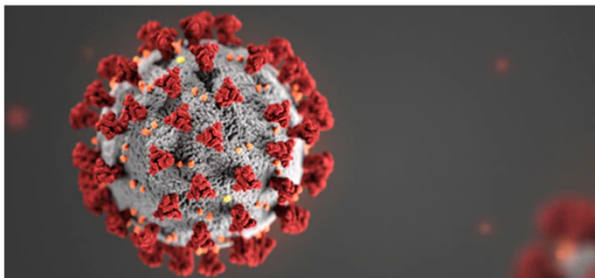
Objectives

- Explain permitted disclosures to public health authorities.
- Discuss the use of telehealth and cybersecurity risks related to COVID-19.

4

OCR GUIDANCE AND ENFORCEMENT DISCRETIONS

HIPAA, Civil Rights, and COVID-19



We are empowering medical providers to serve patients wherever they are during this national public health emergency. We are especially concerned about reaching those most at risk, including older persons and persons with disabilities. – Roger Severino, OCR Director.

During the COVID-19 public health emergency, the HHS Office for Civil Rights (OCR) has provided guidance that helps explain civil rights laws as well as how the HIPAA Privacy Rule allows patient information to be shared in the outbreak of infectious disease and to assist patients in receiving the care they need.

5

COVID-19 and Public Health Services

PHI can be shared, without a patient's permission:

- *with a public health authority*
- *to notify a patient that (s)he has been exposed to a communicable disease*

6

COVID-19 and Public Health Services

Verify the identity of a public health official requesting PHI:

- *In person: an agency ID, other official credentials, or other proof of government status*
- *In writing: the request should be on appropriate government letterhead*
- *Via phone: ask for the request to be sent in writing before making a disclosure.*

Call the government agency for confirmation if you are unsure.

7

OCR GUIDANCE & ENFORCEMENT DISCRETION

- Empowers first responders and others who receive protected health information about individuals who have tested positive or been exposed to COVID-19 to help keep both first responders and the public safe.
- Enforcement Discretion to Allow Uses and Disclosures of Protected Health Information by Business Associates for Public Health and Health Oversight Activities During The COVID-19 Nationwide Public Health Emergency.
 - *EHR vendors*

8



9

OCR ENFORCEMENT DESCRETION - TELEHEALTH

We are empowering medical providers to serve patients wherever they are during this national public health emergency. We are especially concerned about reaching those most at risk, including older persons and persons with disabilities. – Roger Severino, OCR Director.

A health care provider, in the exercise of their professional judgement, can examine a patient exhibiting COVID- 19 symptoms using a video chat application connecting the provider's or patient's phone or desktop computer in order to assess a greater number of patients while limiting the risk of infection of other persons who would be exposed from an in-person consultation.

10

Telehealth

Requires a BAA and sufficient security controls to meet HIPAA requirements. Treat appointments like any other patient encounter – in a private area away from others.

Examples:

- Skype for Business (Microsoft Teams)
- Updox
- VSee
- GoToMeeting
- Zoom for Healthcare
- Spruce Health Care Messenger
- Doxy.me
- Google G Suite Hangouts Meet

11

Telehealth

The Office for Civil Rights (OCR) at the Department of Health and Human Services (HHS) is allowing the **short-term** use of certain applications that do not meet HIPAA security standards. This is for a limited time in order to support response to COVID-19.

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

See today's handouts for basic security tips and resources.

12

Telehealth

This does *not* include applications that are public facing like the following:

Never Use

- Facebook Live
- Twitch
- TikTok

13

Telehealth

Ask a patient about their comfort using technology and what they have available to them when scheduling the appointment.

Check state telehealth consent requirements

(links available in handouts)

14



15

COVID-19 Security Risks

- *Phone*
- *Email*
- *Text*
- *Social media posts*

- *Authority*
- *Emotion*
- *Urgency*
- *Scarcity*

16

COVID-19 Security Risks

Some COVID-19 tracking apps on Android are ransomware viruses

One is called "CovidLock" and it denies access to the entire device and information until the ransom is paid.

17

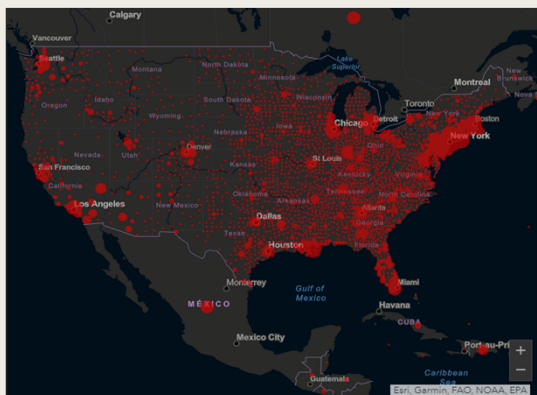
COVID-19 Security Risks

Phishing email and text message scams have infected computer systems and stolen financial information from individuals and businesses related to:

- *PPE*
- *Screening tests*
- *Charitable donations (money and medical supplies)*
- *Fake invoices and order form attachments*
- *Government business loans and stimulus checks*

18

COVID-19 Security Risks



FAKE MAPS & WEBSITES

A user clicks on a map (usually posted in a social media application), malware is downloaded to the user's computer or device that steals usernames, passwords, and financial information.

19

Healthcare is a Target

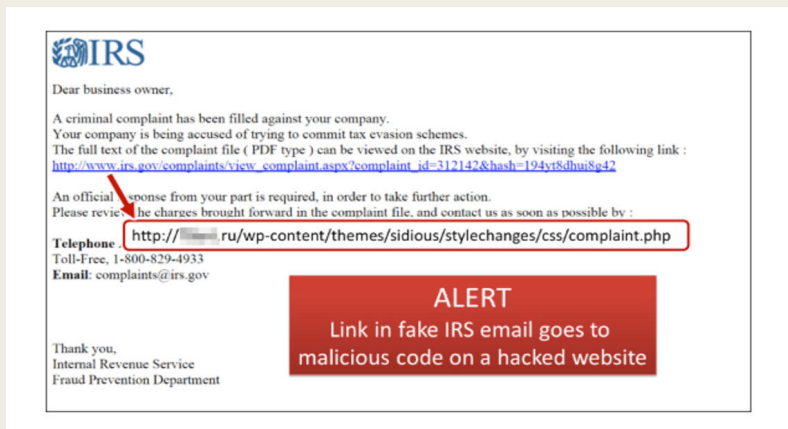
- A patient record includes medical, demographic, financial, and insurance information.
- Most valuable information on the dark web. \$1,000 + per record



20

COVID-19 Security Risks What Can We Do?

- Be suspicious of links in emails, text messages, **social media posts**, and email attachments.



21

COVID-19 Security Risks What Can We Do?

- Do *not* provide usernames, passwords, or financial information to anyone unless you have verified their identity, or you have initiated contact.
 1. For example, the IRS will not email or call you for your SSN, they communicate via the USPS.
 2. Your bank will not email or call you for your account password or PIN.
- Change your passwords now if you haven't in the last 90 days.
- Check with IT to be sure security and software updates are current.
- Avoid downloading internet browser plug-ins.
- Visit **trusted websites** for current information on COVID-19 and related issues.

22

TMC RESOURCE PAGE



TMC 888.862.6742
TOTAL MEDICAL COMPLIANCE

[LOGIN TO ONLINE TRAINING](#)
[NEWSLETTER](#)
[ONLINE STORE](#)
[FREE QUOTE](#)
[CLIENT LOGIN](#)

TMC keeping you updated on COVID - 19
Infection Control for Dental Practices and Medical Practices

[SEE CORONAVIRUS RESOURCES & UPDATES](#)

23

Good to Know

- A copy of handouts will be emailed along with the CE document.
- Continuing education documents only for the live webinar will be provided by THURSDAY, April 16, 2020.
- The webinar is being recorded and will be on the [TMC COVID - 19 Resource Page](#)

24

Thank you!

Karen Gregory, RN
Director of Compliance and Education

Abby Mitchell, CHPC, CHC, HCISPP, CRISC
Senior Compliance Specialist

Service@totalmedicalcompliance.com

888.862.6742