ARIZONA TELEMEDICINE PROGRAM

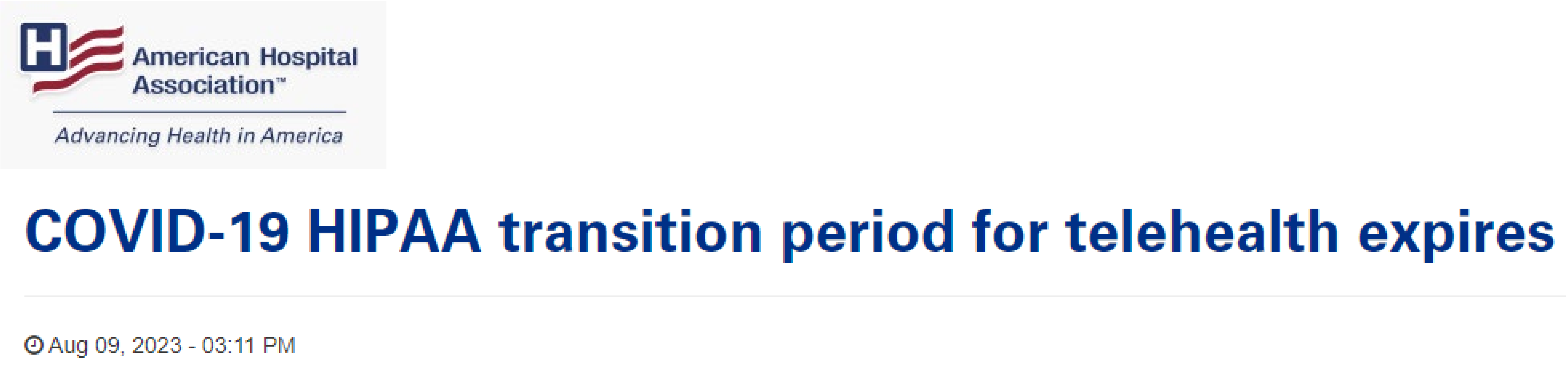
SOUTHWEST TRC TELEHEALTH RESOURCE CENTER™

Telemedicine and Telehealth Privacy and Cybersecurity

Michael Holcomb, BS
Interim Director & Associate Director, Information Technology
mholcomb@telemedicine.arizona.edu

Disclaimer

- Any information related in this presentation is not legal advice and is intended for educational purposes only.
- Consultation with qualified cybersecurity and legal professionals is recommended.
- No conflicts of interest to disclose.



American Hospital Association™

Advancing Health in America

COVID-19 HIPAA transition period for telehealth expires

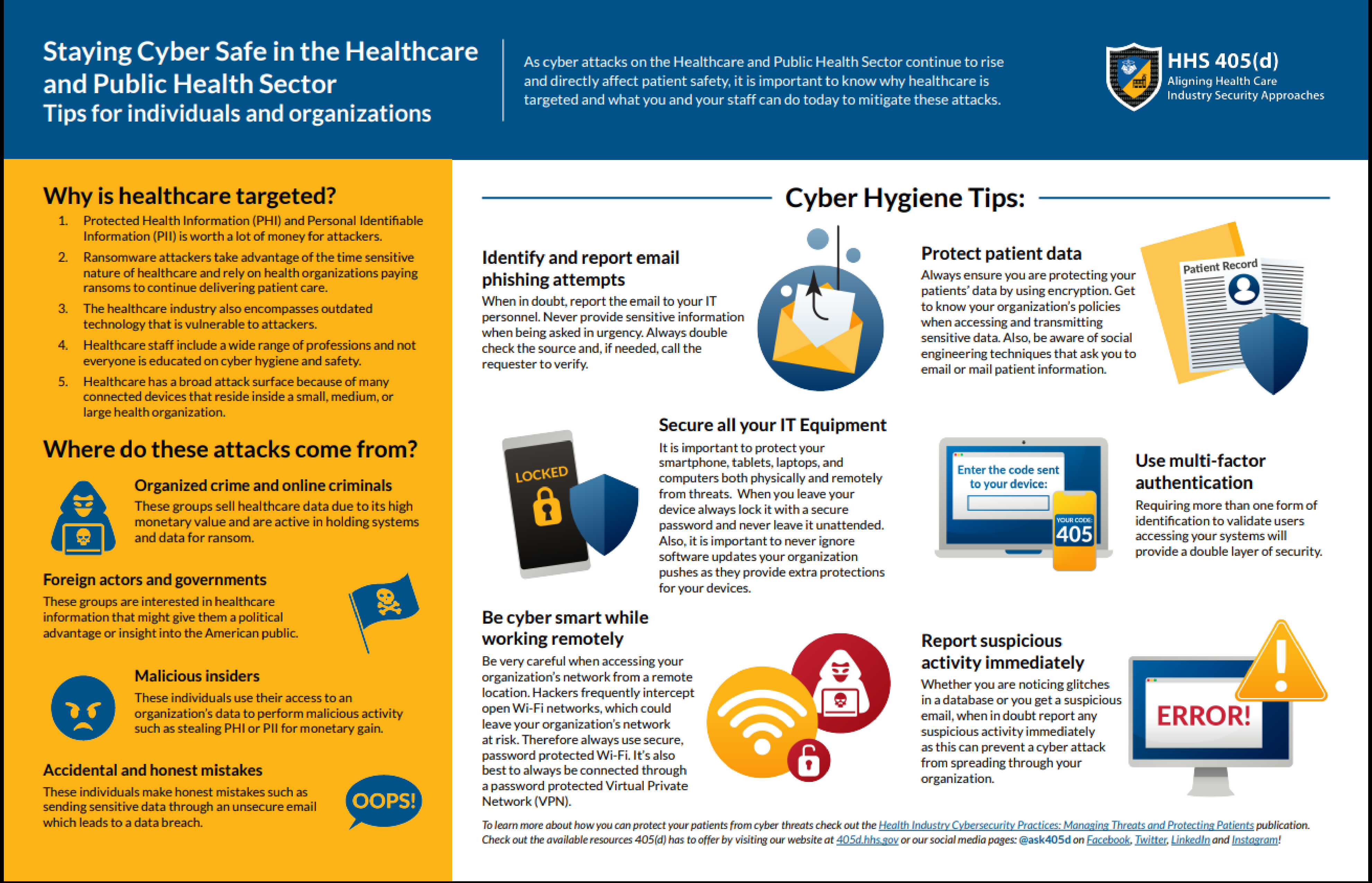
Aug 09, 2023 - 03:11 PM

“Health care providers must comply with the HIPAA rules with respect to telehealth effective Aug. 9 at 11:59 p.m., when the 90-day enforcement discretion period announced in April expires. The Department of Health and Human Services’ Office for Civil Rights implemented a HIPAA enforcement discretion policy for telehealth during the COVID-19 public health emergency, which ended May 11. This provided enforcement discretion to not impose penalties for HIPAA violations against covered health care providers in connection with their good faith provision of telehealth using non-public facing remote communications technologies during the PHE. Providers then had a 90-day transition period to come into compliance…”

https://www.aha.org/news/headline/2023-08-09-covid-19-hipaa-transition-period-telehealth-expires

Telemedicine and Telehealth Privacy and Cybersecurity Outline

- Why is healthcare a target for cyber attacks?
- Types of telemedicine and telehealth communications
- Privacy and cybersecurity considerations
- Health information privacy and security laws, risks, and example types of breaches
- Healthcare is designated as critical infrastructure
- Examples of breaches involving telehealth and/or healthcare orgs
- Information security
  - What is it? How much is needed? How to achieve it?
- Healthcare information security resources



Staying Cyber Safe in the Healthcare and Public Health Sector
Tips for individuals and organizations

As cyber attacks on the Healthcare and Public Health Sector continue to rise and directly affect patient safety, it is important to know why healthcare is targeted and what you and your staff can do today to mitigate these attacks.

HHS 405(d)
Aligning Health Care Industry Security Approaches

Why is healthcare targeted?

1. Protected Health Information (PHI) and Personal Identifiable Information (PII) is worth a lot of money for attackers.
2. Ransomware attackers take advantage of the time sensitive nature of healthcare and rely on health organizations paying ransoms to continue delivering patient care.
3. The healthcare industry also encompasses outdated technology that is vulnerable to attackers.
4. Healthcare staff include a wide range of professions and not everyone is educated on cyber hygiene and safety.
5. Healthcare has a broad attack surface because of many connected devices that reside inside a small, medium, or large health organization.

Where do these attacks come from?

Organized crime and online criminals
These groups sell healthcare data due to its high monetary value and are active in holding systems and data for ransom.

Foreign actors and governments
These groups are interested in healthcare information that might give them a political advantage or insight into the American public.

Malicious insiders
These individuals use their access to an organization's data to perform malicious activity such as stealing PHI or PII for monetary gain.

Accidental and honest mistakes
These individuals make honest mistakes such as sending sensitive data through an unsecure email which leads to a data breach.

Cyber Hygiene Tips:

Identify and report email phishing attempts
When in doubt, report the email to your IT personnel. Never provide sensitive information when being asked in urgency. Always double check the source and, if needed, call the requester to verify.

Protect patient data
Always ensure you are protecting your patients' data by using encryption. Get to know your organization's policies when accessing and transmitting sensitive data. Also, be aware of social engineering techniques that ask you to email or mail patient information.

Secure all your IT Equipment
It is important to protect your smartphone, tablets, laptops, and computers both physically and remotely from threats. When you leave your device always lock it with a secure password and never leave it unattended. Also, it is important to never ignore software updates your organization pushes as they provide extra protections for your devices.

Use multi-factor authentication
Requiring more than one form of identification to validate users accessing your systems will provide a double layer of security.

Be cyber smart while working remotely
Be very careful when accessing your organization's network from a remote location. Hackers frequently intercept open Wi-Fi networks, which could leave your organization's network at risk. Therefore always use secure, password protected Wi-Fi. It's also best to always be connected through a password protected Virtual Private Network (VPN).

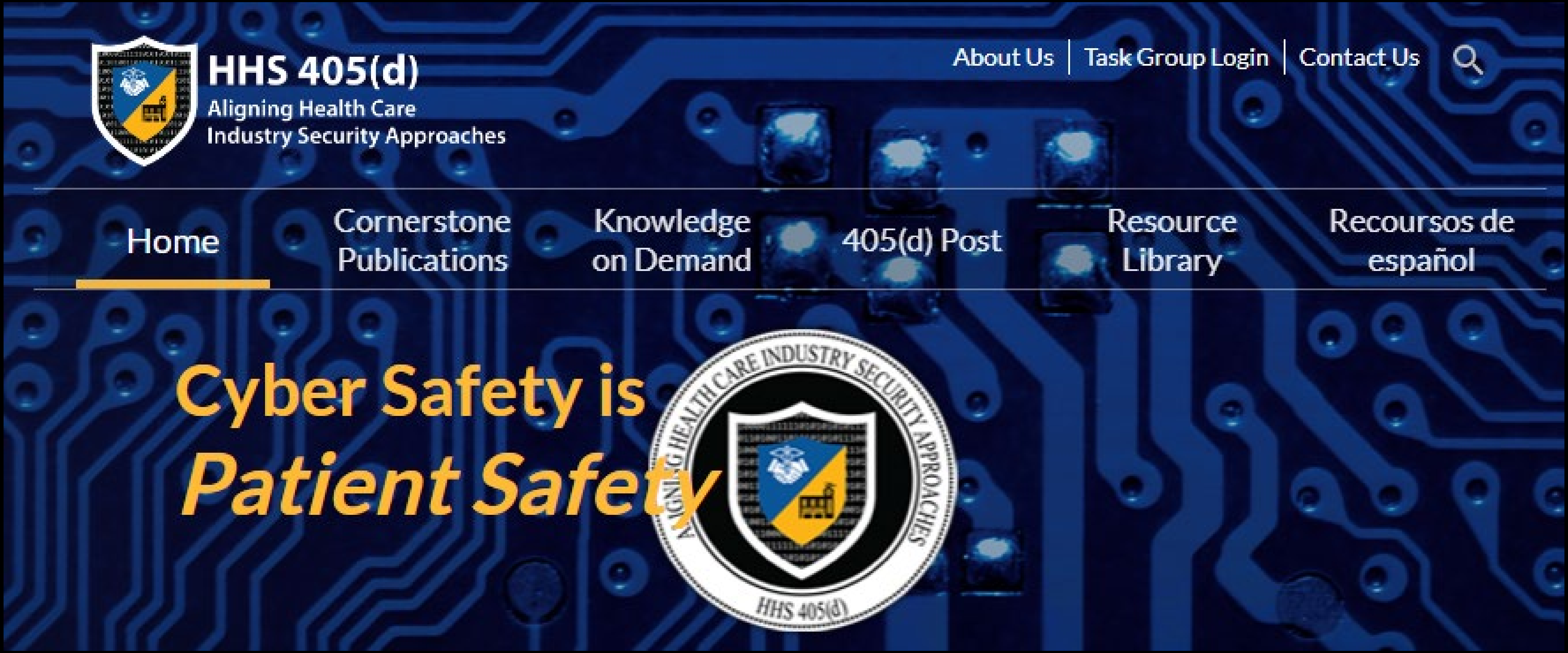
Report suspicious activity immediately
Whether you are noticing glitches in a database or you get a suspicious email, when in doubt report any suspicious activity immediately as this can prevent a cyber attack from spreading through your organization.

To learn more about how you can protect your patients from cyber threats check out the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication. Check out the available resources 405(d) has to offer by visiting our website at 405d.hhs.gov or our social media pages: @ask405d on Facebook, Twitter, LinkedIn and Instagram!

https://405d.hhs.gov/Documents/405d-Infographic-StayingCyberSafeInHPH.pdf

Arizona Telemedicine Program

Southwest Telehealth Resource Center TRC



HHS 405(d)
Aligning Health Care
Industry Security Approaches

About Us | Task Group Login | Contact Us

https://405d.hhs.gov/

Types of Telemedicine and Telehealth Communications (selected)

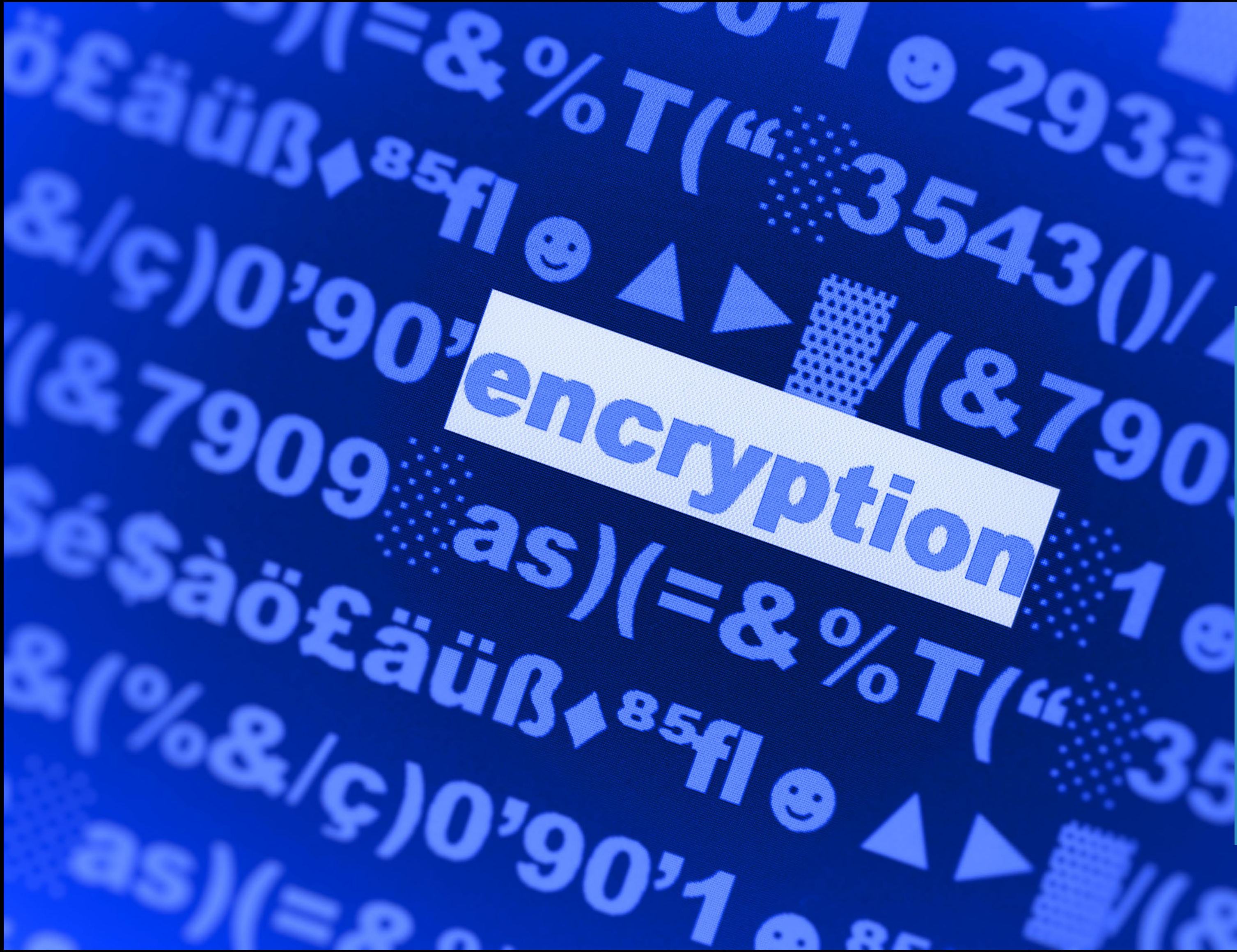
- Real-time interactive (synchronous)
  - Video calls
  - Audio only
- Store and forward (asynchronous)
- Remote auscultation using electronic stethoscopes (sync or async)
- Remote patient monitoring (RPM)
- Secure text messaging
- Artificial intelligence (AI) assisted triage and consultation

Telemedicine and Telehealth Privacy Considerations

- Compliance with regulations
- Good business practice
- Patient consent
- Establish and maintain trust between providers and patients
- Location/environment considerations
- Secure communications
- All forms of protected health information (PHI) need to be secured and protected from unauthorized uses and disclosures at all times
  - **Inventory of PHI is key to understanding and informing risk assessment and mitigation efforts**

Telemedicine and Telehealth Cybersecurity Considerations (continued)

- Protect patients' privacy and safety
- Compliance with regulations
- Good business practice
- Prevent and mitigate cyber attacks and data privacy breaches
- Protect continuity of operations
- Prevent tampering with data and medical devices

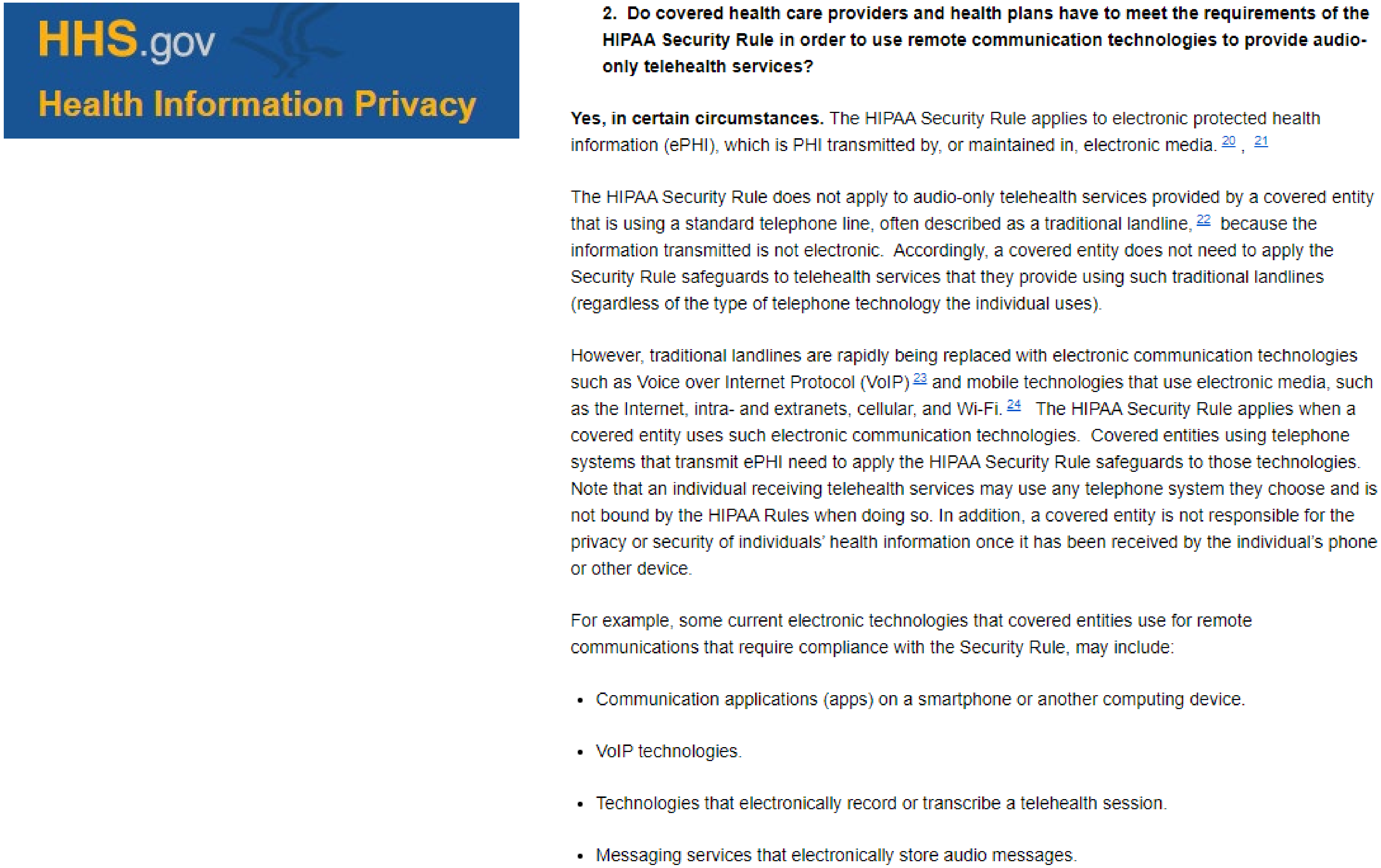


Bofotolux/stock.adobe.com

MQ-Illustrations/stock.adobe.com

Telemedicine and Telehealth Cybersecurity Considerations (continued)

- Secure handling of regulated and sensitive information
  - Encrypt communications and data in motion
    - Encrypted virtual private networks
    - Encrypted / Secure email
  - Encrypt data at rest while in storage or archive status
    - Full disk or device encryption
  - Harden devices, operating systems and software applications
    - Central policy management , mobile device management
  - Voice over IP is an electronic voice communications system and is subject to the HIPAA security rule when used for communications contain protected health information



HHS.gov
Health Information Privacy

2. Do covered health care providers and health plans have to meet the requirements of the HIPAA Security Rule in order to use remote communication technologies to provide audio-only telehealth services?

Yes, in certain circumstances. The HIPAA Security Rule applies to electronic protected health information (ePHI), which is PHI transmitted by, or maintained in, electronic media. [20] , [21]

The HIPAA Security Rule does not apply to audio-only telehealth services provided by a covered entity that is using a standard telephone line, often described as a traditional landline, [22] because the information transmitted is not electronic. Accordingly, a covered entity does not need to apply the Security Rule safeguards to telehealth services that they provide using such traditional landlines (regardless of the type of telephone technology the individual uses).

However, traditional landlines are rapidly being replaced with electronic communication technologies such as Voice over Internet Protocol (VoIP) [23] and mobile technologies that use electronic media, such as the Internet, intra- and extranets, cellular, and Wi-Fi. [24] The HIPAA Security Rule applies when a covered entity uses such electronic communication technologies. Covered entities using telephone systems that transmit ePHI need to apply the HIPAA Security Rule safeguards to those technologies. Note that an individual receiving telehealth services may use any telephone system they choose and is not bound by the HIPAA Rules when doing so. In addition, a covered entity is not responsible for the privacy or security of individuals' health information once it has been received by the individual's phone or other device.

For example, some current electronic technologies that covered entities use for remote communications that require compliance with the Security Rule, may include:

- Communication applications (apps) on a smartphone or another computing device.
- VoIP technologies.
- Technologies that electronically record or transcribe a telehealth session.
- Messaging services that electronically store audio messages.

https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-audio-telehealth/index.html

Telemedicine and Telehealth Cybersecurity Considerations

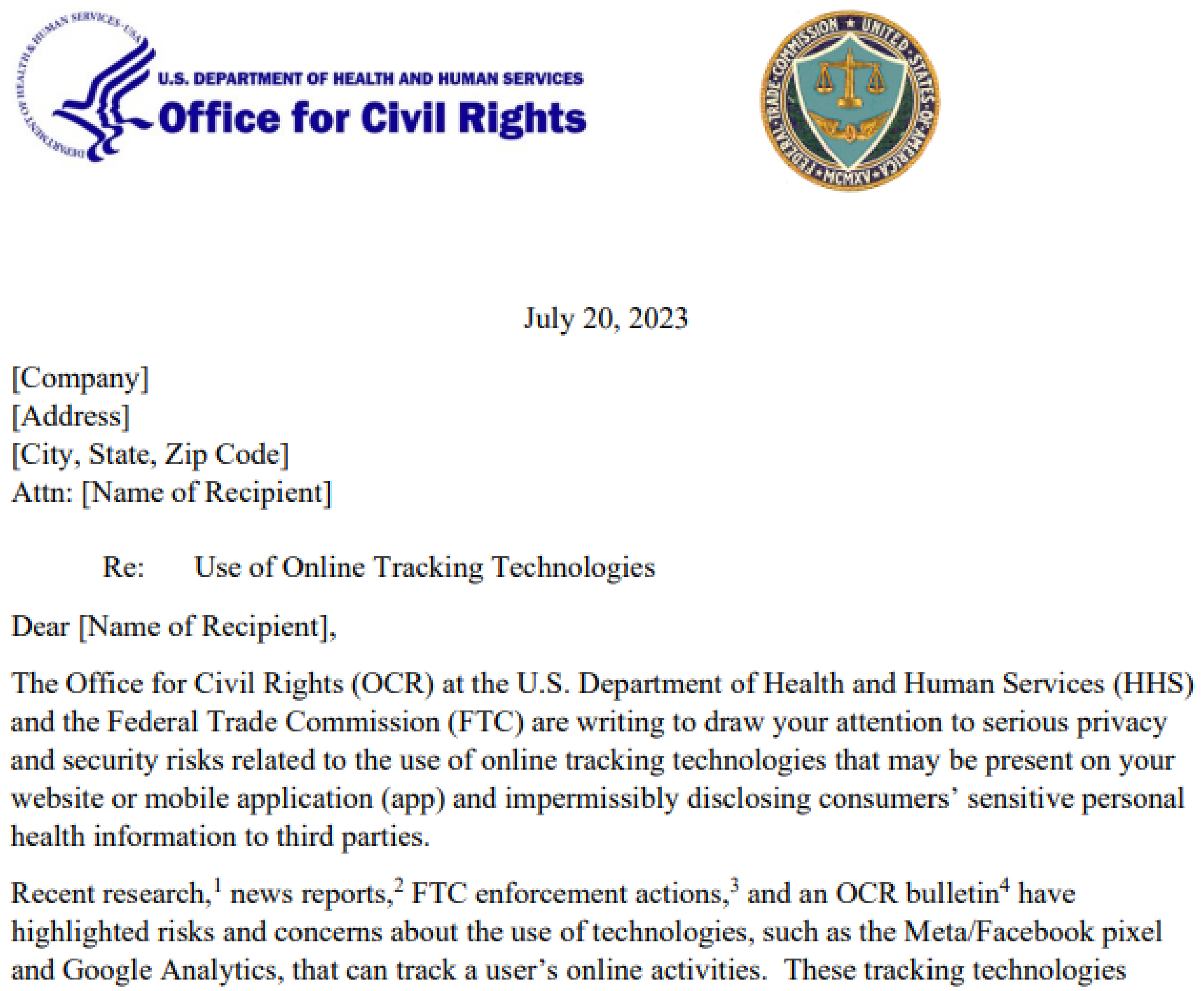
- Use applications and devices that are designed to support HIPAA compliance
- Train staff in the secure use of the organization's approved technologies and also about cybersecurity awareness
- **Risk assessment is key to achieving effective security**
- **Business associate agreements are essential when 3rd parties will have access to PHI**

ZETHA_WORK/stock.adobe.com

Health Information Privacy: Laws, Risks, and Breaches

Patient and Consumer Health Information Privacy Laws	Protected Health Information Privacy Risks	Examples of Protected Health Information Privacy Breach Causes and Vectors
FTC Act 1914	Hacking	Human behavior: error, social engineering, privilege misuse, insider threats
HIPAA 1996	IT Incidents	Business email compromise: phishing
COPPA 1998	Unauthorized Access	Ransomware
HITECH Act 2009	Unauthorized Disclosure	IT system misconfiguration
HIPAA Omnibus Rule 2013	Loss	Failure to assess and manage risk
State privacy and data security laws that exceed, but are not contrary to, federal laws	Theft	Sharing PHI with 3rd parties/vendors: without a BAA, without vetting information security practices
	Improper Disposal	Exploitation of software and hardware vulnerabilities
		Loss or theft of unencrypted data

FTC and US Department of HHS Office for Civil Rights Joint Letter to ~130 hospital systems July 20, 2023



U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights

July 20, 2023

[Company]
[Address]
[City, State, Zip Code]
Attn: [Name of Recipient]

Re: Use of Online Tracking Technologies

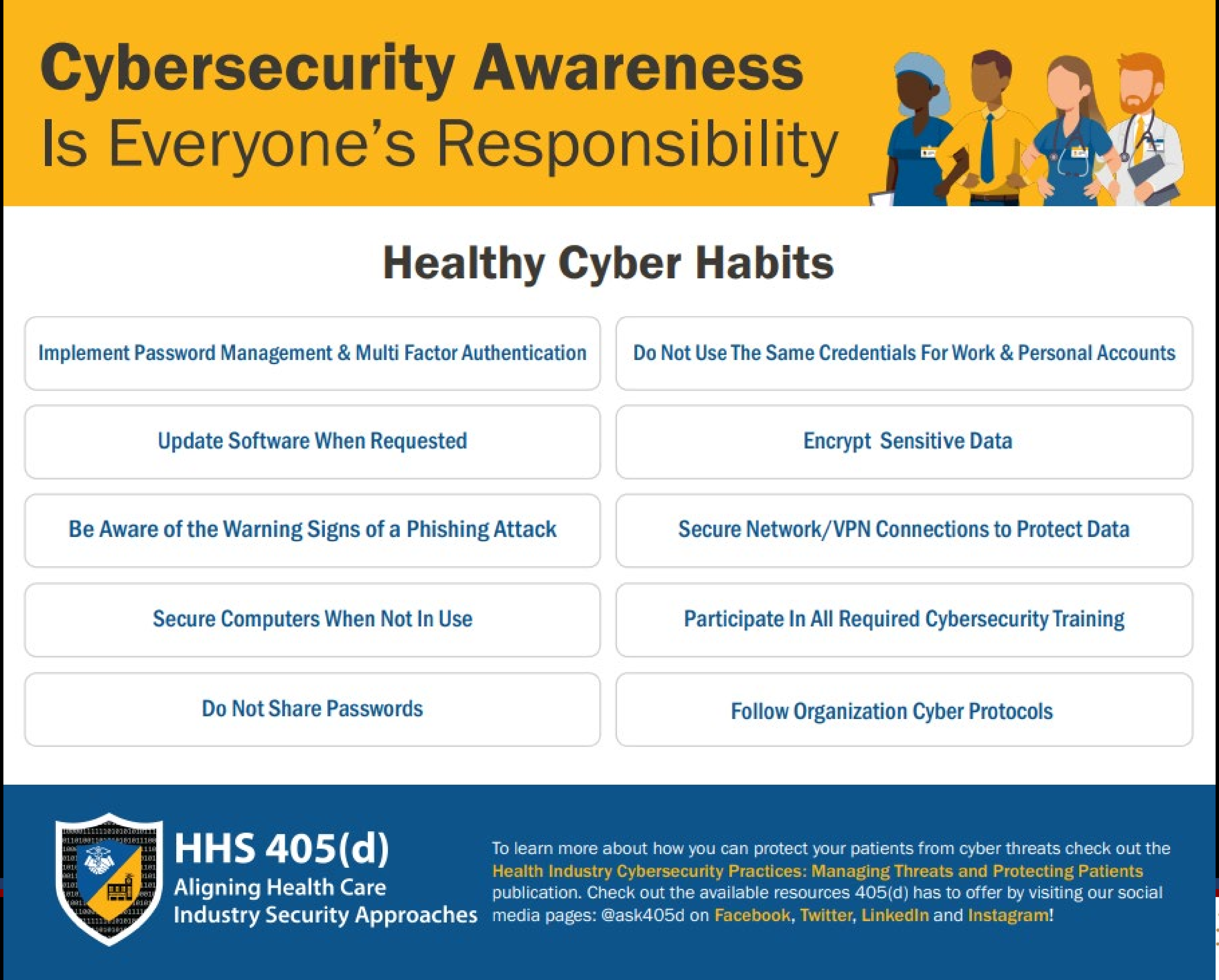
Dear [Name of Recipient],

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC) are writing to draw your attention to serious privacy and security risks related to the use of online tracking technologies that may be present on your website or mobile application (app) and impermissibly disclosing consumers' sensitive personal health information to third parties.

Recent research,[1] news reports,[2] FTC enforcement actions,[3] and an OCR bulletin[4] have highlighted risks and concerns about the use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user's online activities. These tracking technologies

https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf

Natassia/stock.adobe.com



Cybersecurity Awareness Is Everyone’s Responsibility

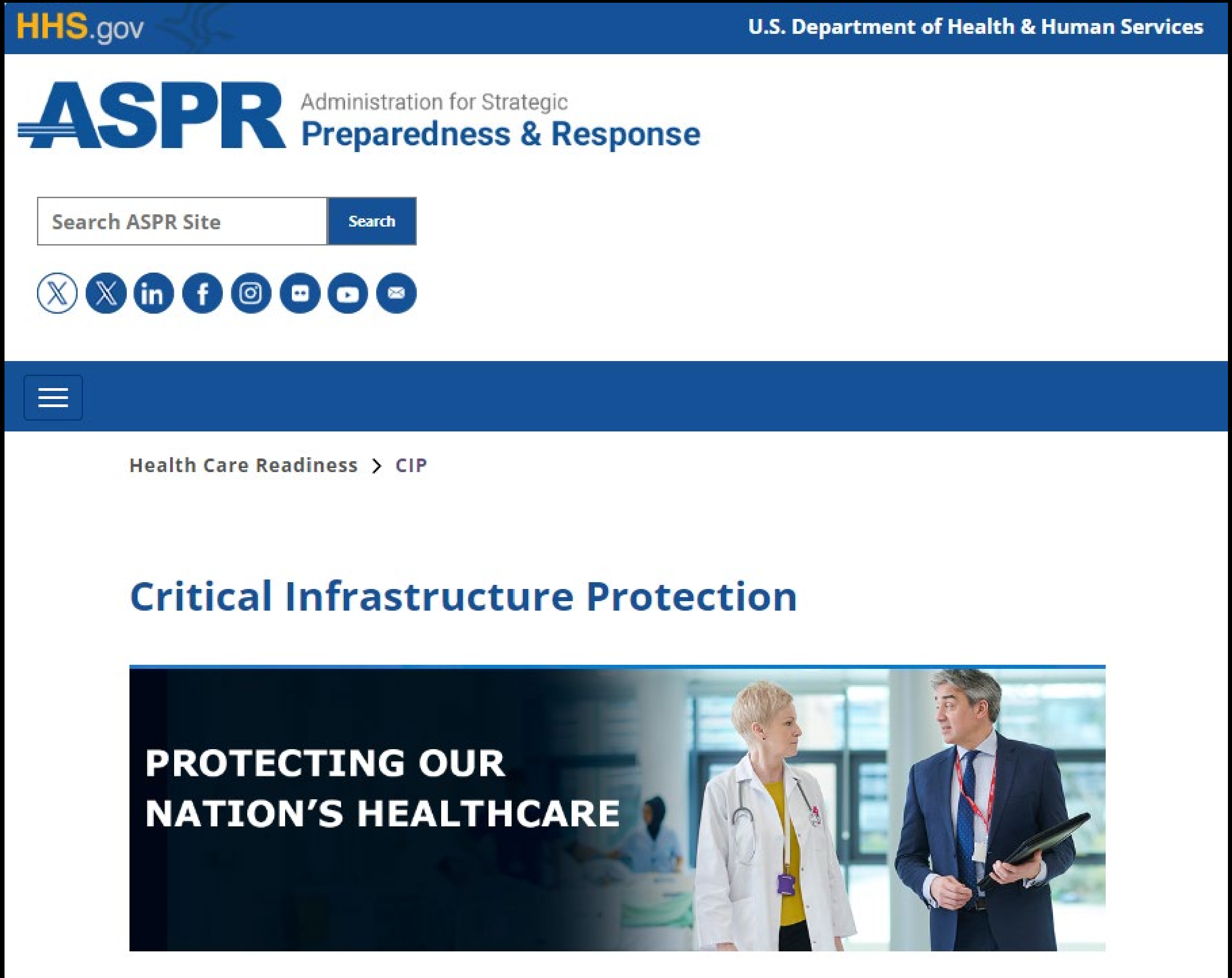
Healthy Cyber Habits

Implement Password Management & Multi Factor Authentication	Do Not Use The Same Credentials For Work & Personal Accounts
Update Software When Requested	Encrypt Sensitive Data
Be Aware of the Warning Signs of a Phishing Attack	Secure Network/VPN Connections to Protect Data
Secure Computers When Not In Use	Participate In All Required Cybersecurity Training
Do Not Share Passwords	Follow Organization Cyber Protocols

HHS 405(d)
Aligning Health Care
Industry Security Approaches

To learn more about how you can protect your patients from cyber threats check out the **Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients** publication. Check out the available resources 405(d) has to offer by visiting our social media pages: @ask405d on **Facebook**, **Twitter**, **LinkedIn** and **Instagram**!

https://405d.hhs.gov/Documents/405d-healthy-cyber-habits.pdf


HHS.gov

U.S. Department of Health & Human Services

ASPR Administration for Strategic Preparedness & Response

Health Care Readiness > CIP

Critical Infrastructure Protection

https://aspr.hhs.gov/cip/Pages/default.aspx

Some healthcare breach examples

- 2020: A behavioral telehealth provider's system misconfiguration briefly makes recordings of patients' sessions publicly available online
- 2021: Telehealth platform fixes issue that exposed patient data to 3 external companies
- 2021: Arizona medical center ransomware attack corrupts 35,000 patient records
- 2023: FTC fined two different telehealth providers, one for $1.5 million for failing to comply with the FTC health breach notification rule and the other for $7.8 million for sharing patient information with 3rd parties without consent
- 2023: a telebehavioral health provider disclosed protected health information of more than 3 million patients to third-party platforms without patient consent
- 2024: healthcare claims processing company suffers ransomware attack

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

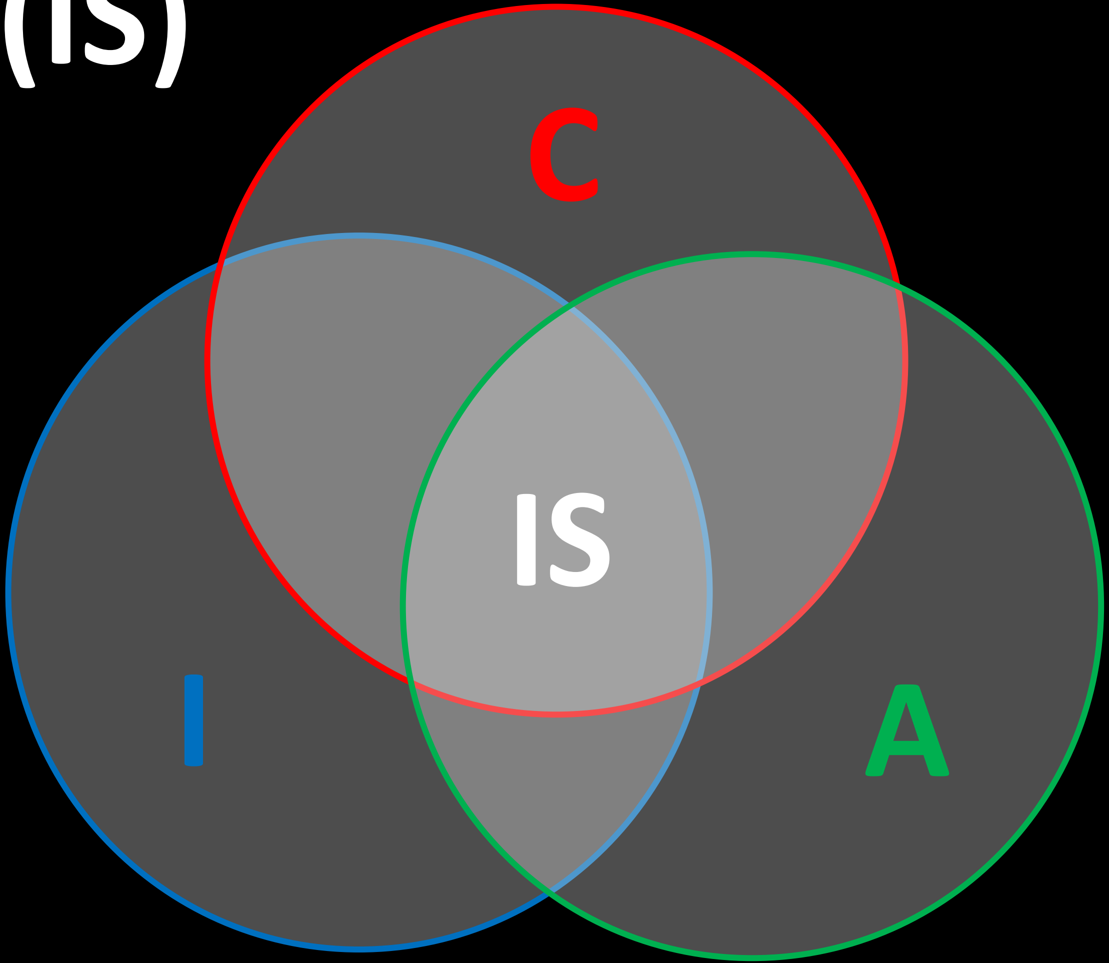
https://www.youtube.com/watch?v=vRG4_kDTxTU

Telehealth: Visit Metacommunications and Metadata

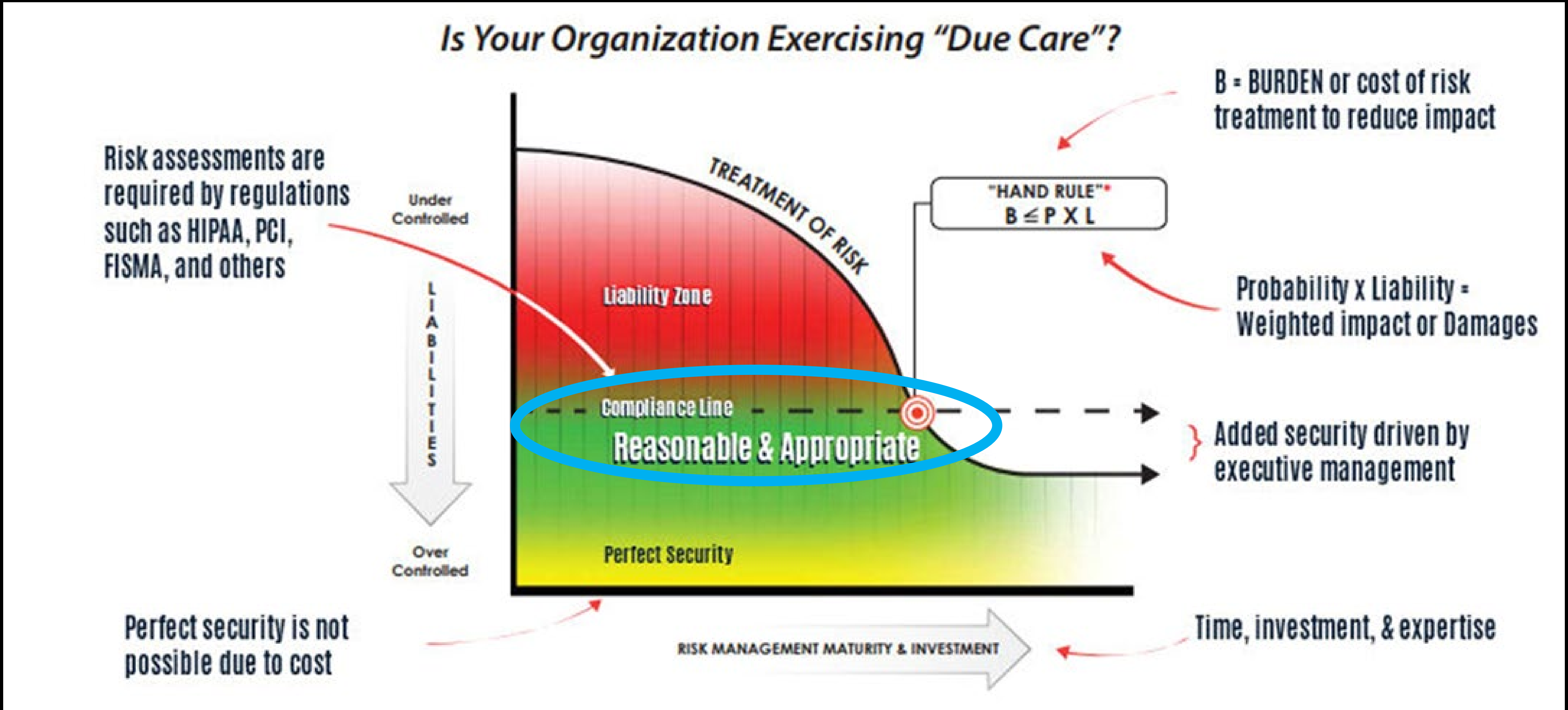
- Data communicated about the telehealth visit
  - Email, text or voice messages containing PII such as scheduling messages
  - Direct links to telehealth visit session
    - Is the same link used for more than one patient?
    - Can someone else who has the link intrude on a live telehealth visit?
- Data logged about the telehealth visit
  - PII or PHI such as patient name, email address, ip address, etc.
  - Is the telehealth visit recorded?
    - By provider?
    - By patient?

Information Security (IS)

- **Confidentiality (C)**
  - Privacy of information is maintained among authorized entities and protected from unauthorized access and use
- **Integrity (I)**
  - Information is accurate, complete, and protected from unauthorized changes
- **Availability (A)**
  - Information access is reliable and timely for authorized users when needed



Halock blog: The Hand Rule: Managing the Upper Limits of Security Costs



Is Your Organization Exercising "Due Care"?

Risk assessments are required by regulations such as HIPAA, PCI, FISMA, and others

B = BURDEN or cost of risk treatment to reduce impact

Probability x Liability = Weighted impact or Damages

Added security driven by executive management

Perfect security is not possible due to cost

Time, investment, & expertise

https://www.halock.com/hand-rule-managing-upper-limits-security-costs/

The NIST Cybersecurity Framework (CSF) 2.0

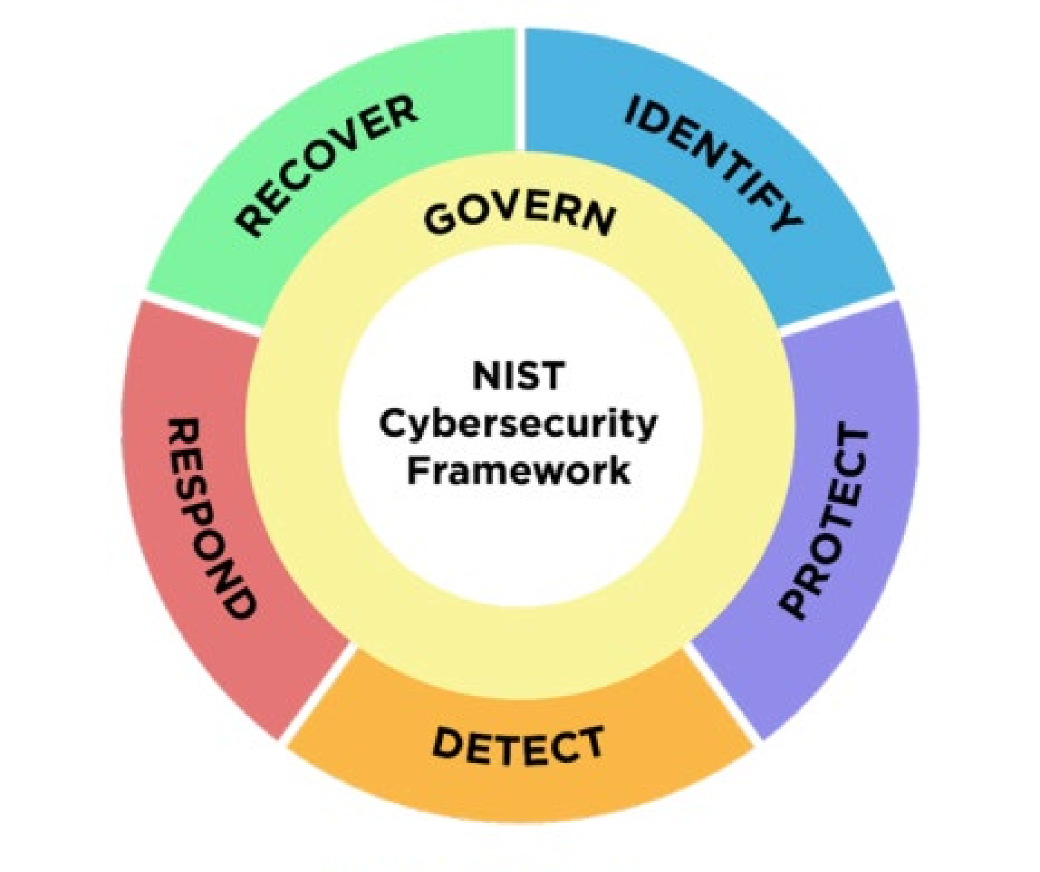
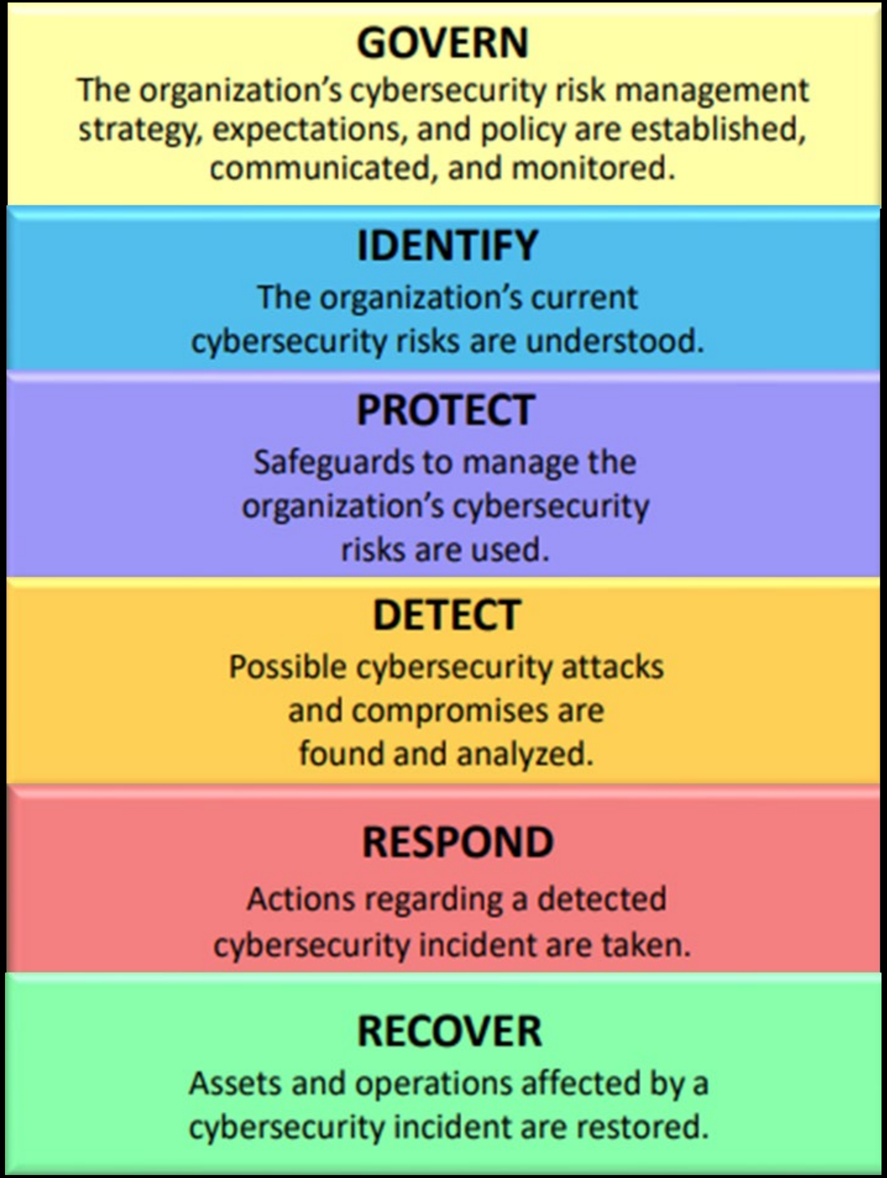


Fig. 2. CSF Functions

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

The NIST CSF 2.0 Functions



GOVERN
The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.

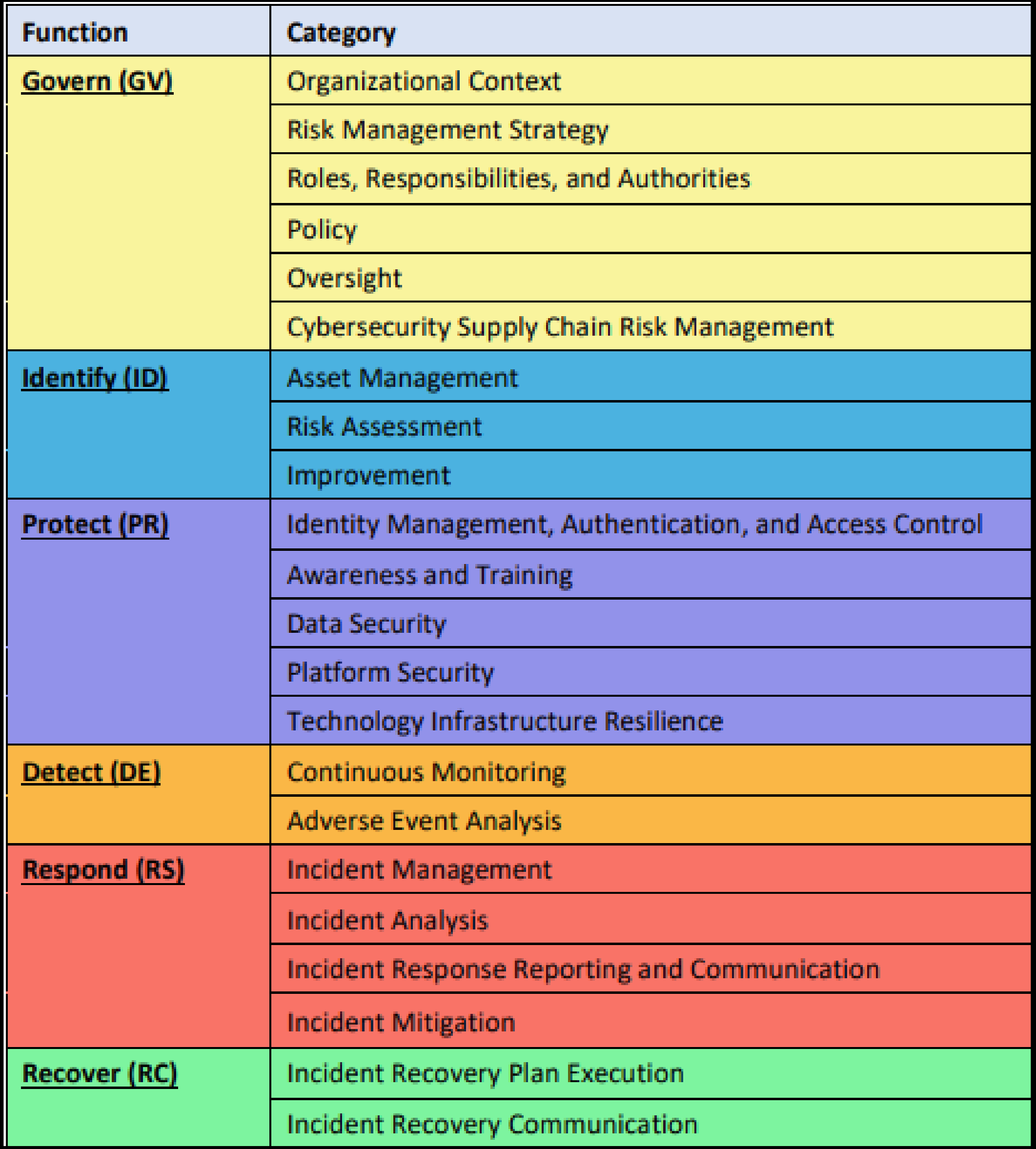
IDENTIFY
The organization's current cybersecurity risks are understood.

PROTECT
Safeguards to manage the organization's cybersecurity risks are used.

DETECT
Possible cybersecurity attacks and compromises are found and analyzed.

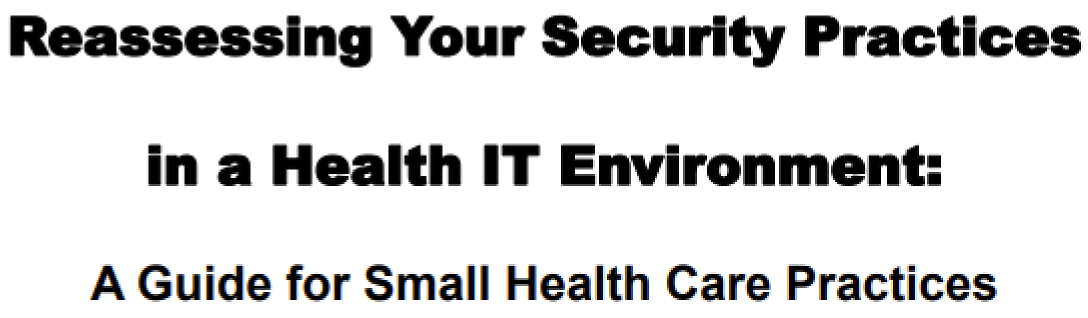
RESPOND
Actions regarding a detected cybersecurity incident are taken.

RECOVER
Assets and operations affected by a cybersecurity incident are restored.



Function	Category
Govern (GV)	Organizational Context
	Risk Management Strategy
	Roles, Responsibilities, and Authorities
	Policy
	Oversight
	Cybersecurity Supply Chain Risk Management
Identify (ID)	Asset Management
	Risk Assessment
	Improvement
Protect (PR)	Identity Management, Authentication, and Access Control
	Awareness and Training
	Data Security
	Platform Security
	Technology Infrastructure Resilience
Detect (DE)	Continuous Monitoring
	Adverse Event Analysis
Respond (RS)	Incident Management
	Incident Analysis
	Incident Response Reporting and Communication
	Incident Mitigation
Recover (RC)	Incident Recovery Plan Execution
	Incident Recovery Communication

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1299.pdf



Reassessing Your Security Practices in a Health IT Environment:

A Guide for Small Health Care Practices

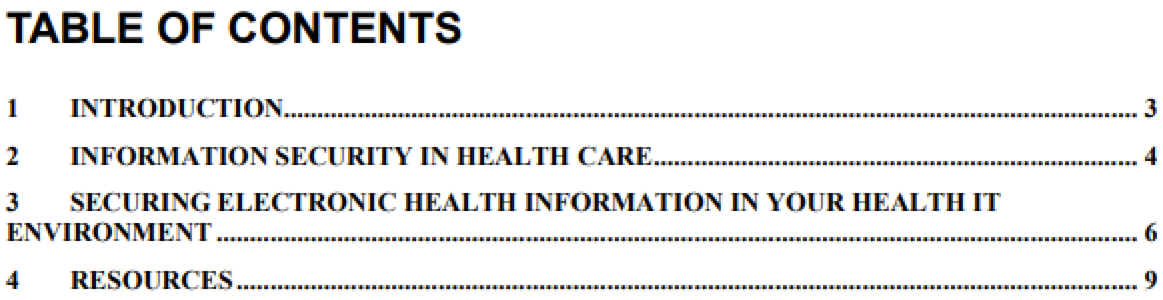
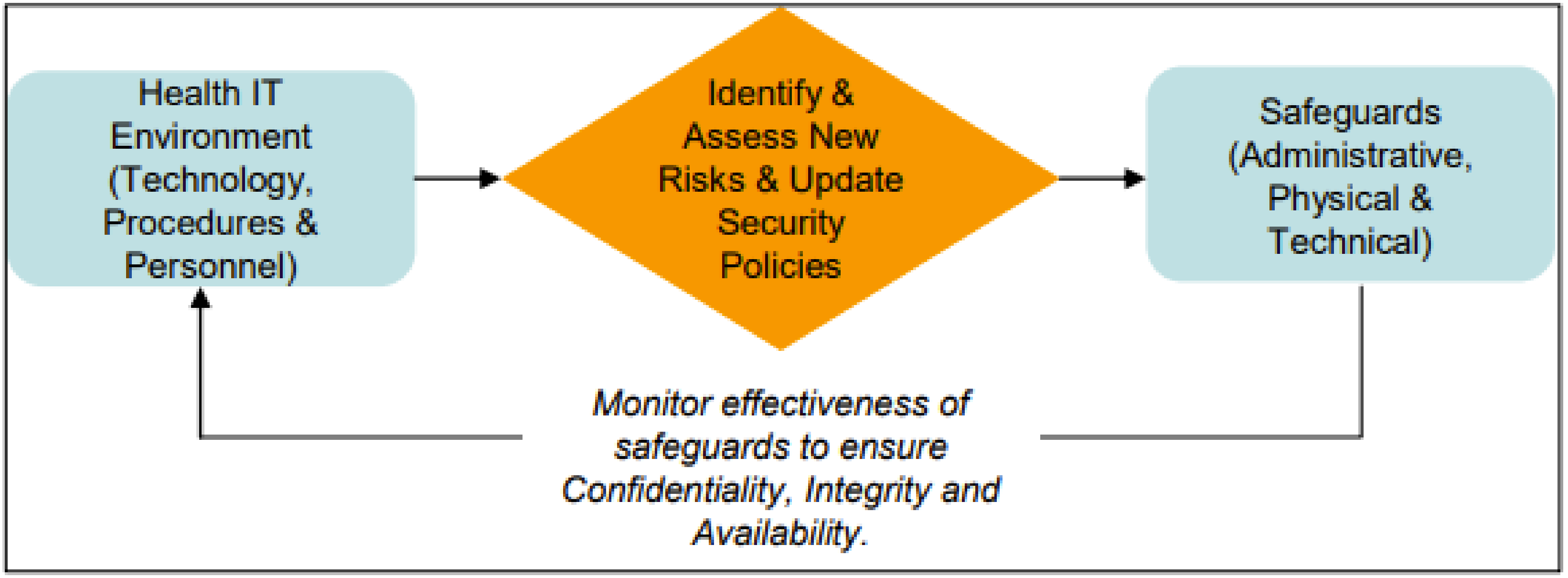


TABLE OF CONTENTS



Health IT Environment (Technology, Procedures & Personnel)
Identify & Assess New Risks & Update Security Policies
Safeguards (Administrative, Physical & Technical)
Monitor effectiveness of safeguards to ensure Confidentiality, Integrity and Availability.

Figure 1: Health Information Security Requires Continual Assessment of Risks to Electronic Health Information

https://www.hhs.gov/sites/default/files/small-practice-security-guide-1.pdf

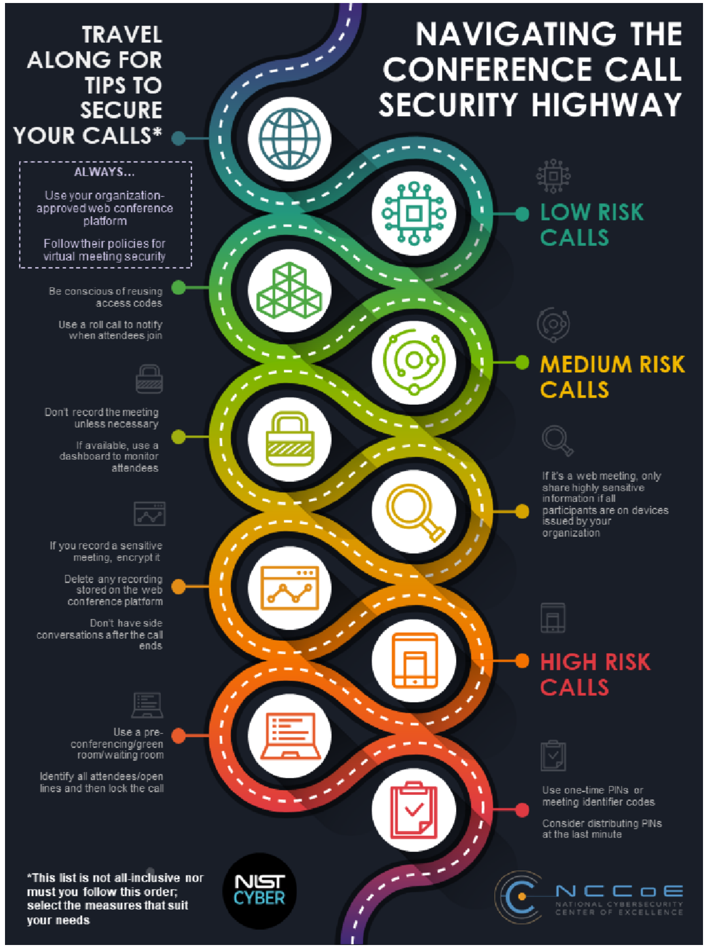
Non-exhaustive list of steps you can take to improve the security of conference calls

"…

- Follow your organization's policies for virtual meeting security.
- Limit reuse of access codes; if you've used the same code for a while, you've probably shared it with more people than you can imagine or recall.
- If the topic is sensitive, use one-time PINs or meeting identifier codes, and consider multi-factor authentication.
- Use a "green room" or "waiting room" and don't allow the meeting to begin until the host joins.
- Enable notification when attendees join by playing a tone or announcing names. If this is not an option, make sure the meeting host asks new attendees to identify themselves.
- If available, use a dashboard to monitor attendees – and identify all generic attendees.
- Don't record the meeting unless it's necessary.
- If it's a web meeting (with video):
    - Disable features you don't need (like chat, file sharing, or screen sharing).
    - Consider using a PIN to prevent someone from crashing your meeting by guessing your URL or meeting ID.
    - Limit who can share their screen to avoid any unwanted or unexpected images. And before anyone shares their screen, remind them not to share sensitive information inadvertently…"

NIST

< CYBERSECURITY INSIGHTS a NIST blog



NAVIGATING THE CONFERENCE CALL SECURITY HIGHWAY

TRAVEL ALONG FOR TIPS TO SECURE YOUR CALLS*

ALWAYS...

Use your organization-approved web conference platform

Follow their policies for virtual meeting security

LOW RISK CALLS

Be conscious of reusing access codes

Use a roll call to notify when attendees join

MEDIUM RISK CALLS

Don't record the meeting unless necessary

If available, use a dashboard to monitor attendees

If it's a web meeting, only share highly sensitive information if all participants are on devices issued by your organization

If you record a sensitive meeting, encrypt it

Delete any recording stored on the web conference platform

Don't have side conversations after the call ends

HIGH RISK CALLS

Use a pre-conferencing/green room/waiting room

Identify all attendees/open lines and then lock the call

Use one-time PINs or meeting identifier codes

Consider distributing PINs at the last minute

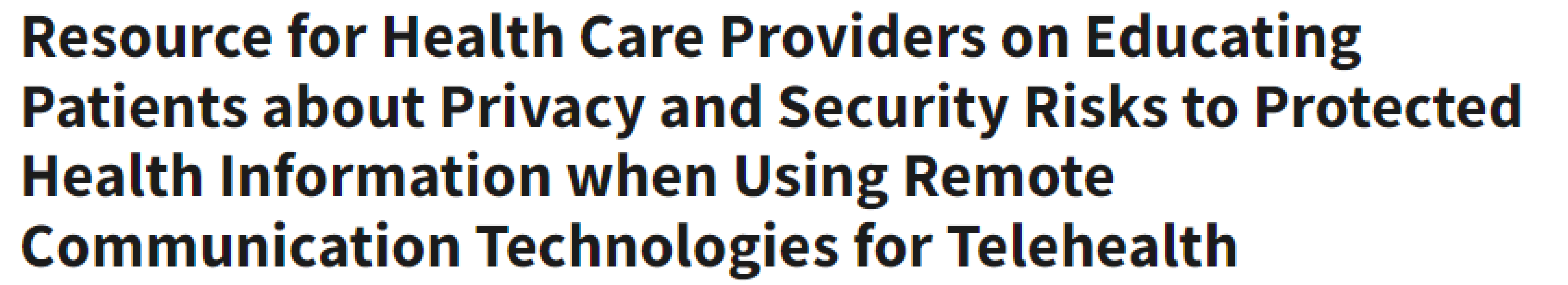
*This list is not all-inclusive nor must you follow this order; select the measures that suit your needs

https://www.nist.gov/blogs/cybersecurity-insights/preventing-eavesdropping-and-protecting-privacy-virtual-meetings

U.S. Department of Health and Human Services

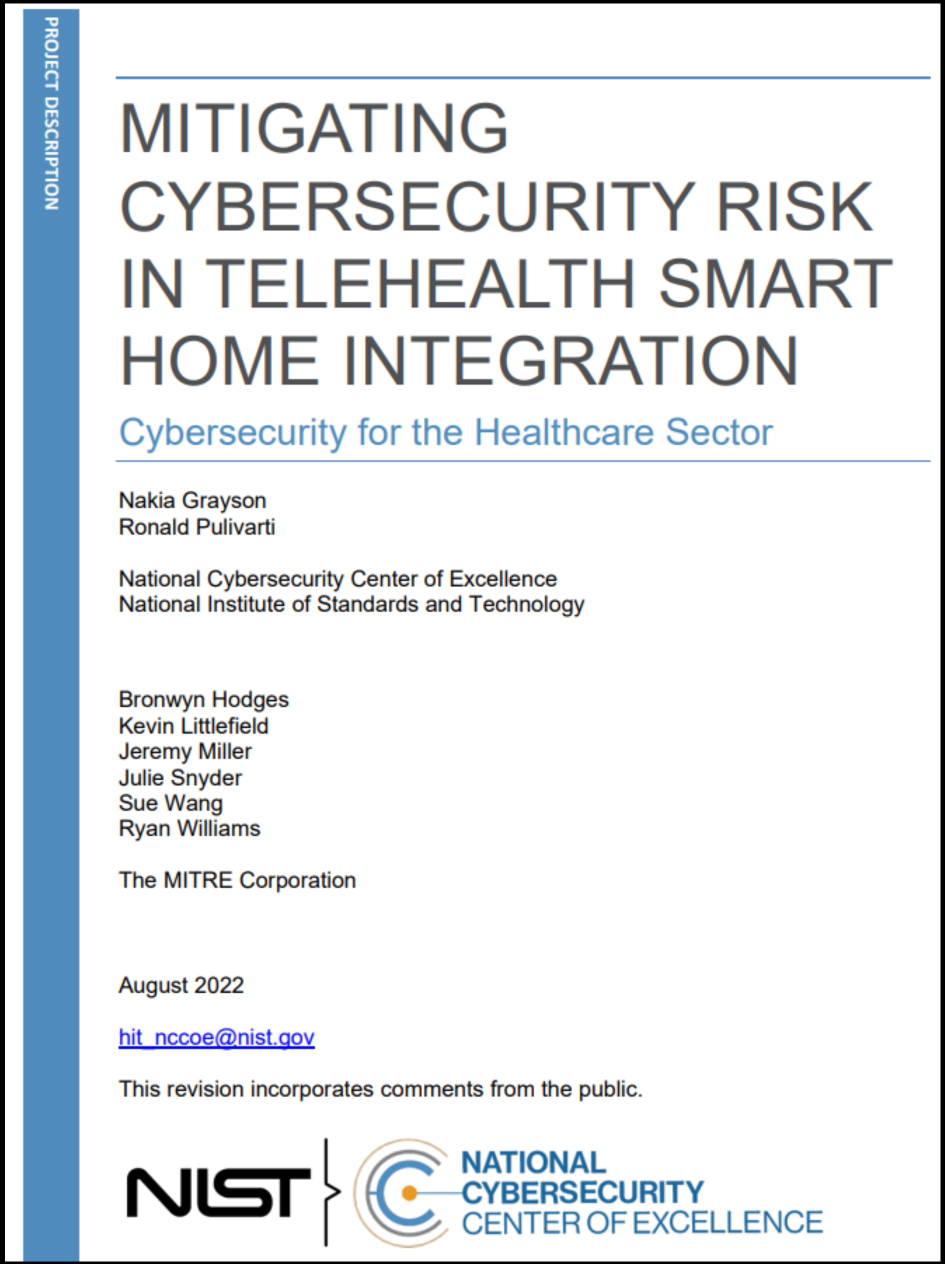
Enhancing the health and well-being of all Americans

Health Information Privacy



Resource for Health Care Providers on Educating Patients about Privacy and Security Risks to Protected Health Information when Using Remote Communication Technologies for Telehealth

https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/resource-health-care-providers-educating-patients/index.html



PROJECT DESCRIPTION

MITIGATING CYBERSECURITY RISK IN TELEHEALTH SMART HOME INTEGRATION

Cybersecurity for the Healthcare Sector

Nakia Grayson
Ronald Pulivarti

National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Bronwyn Hodges
Kevin Littlefield
Jeremy Miller
Julie Snyder
Sue Wang
Ryan Williams

The MITRE Corporation

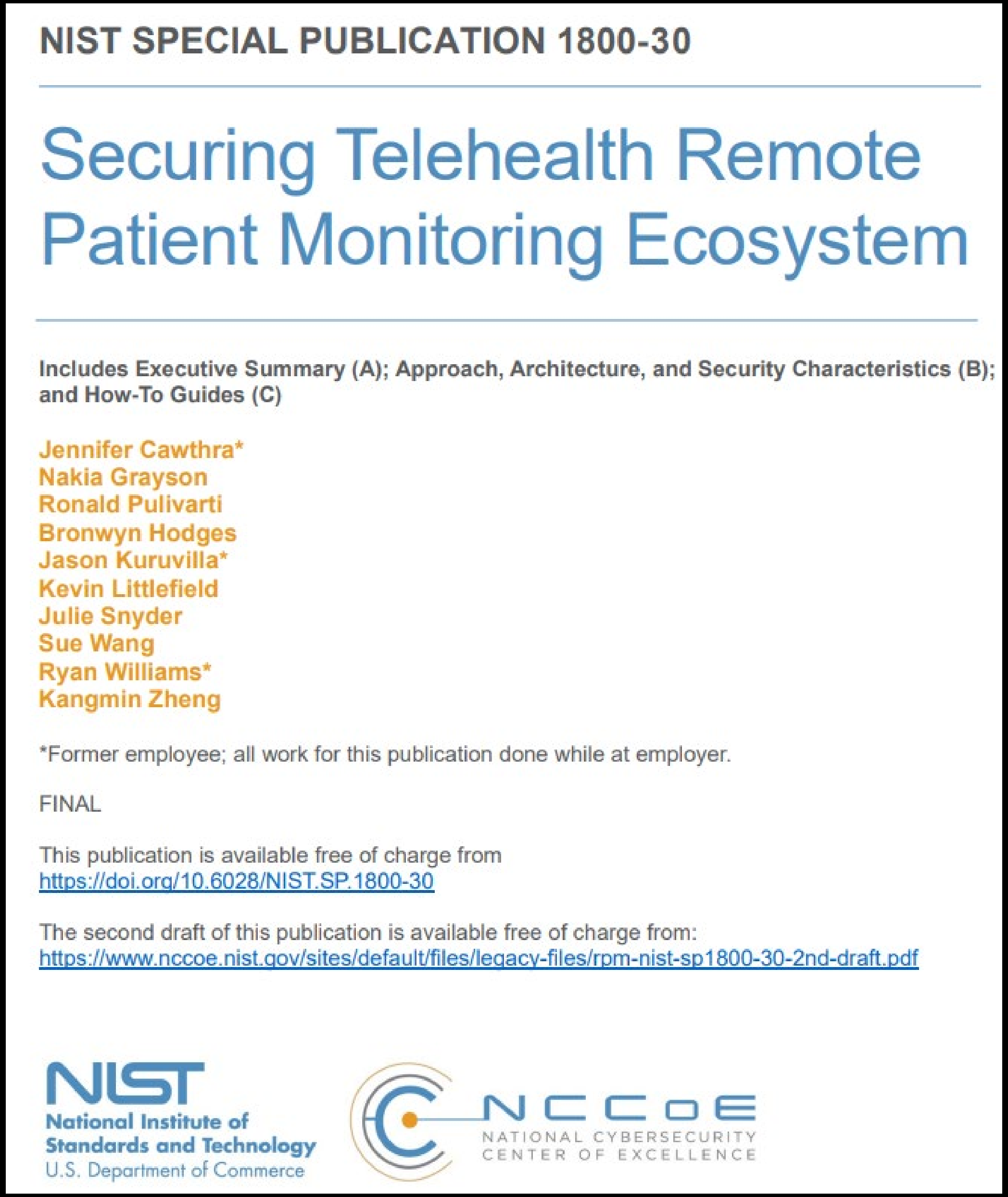
August 2022

hit_nccoe@nist.gov

This revision incorporates comments from the public.

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

https://www.nccoe.nist.gov/sites/default/files/2022-08/hit-shi-project-description-final.pdf



NIST SPECIAL PUBLICATION 1800-30

Securing Telehealth Remote Patient Monitoring Ecosystem

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

Jennifer Cawthra*
Nakia Grayson
Ronald Pulivarti
Bronwyn Hodges
Jason Kuruvilla*
Kevin Littlefield
Julie Snyder
Sue Wang
Ryan Williams*
Kangmin Zheng

*Former employee; all work for this publication done while at employer.

FINAL

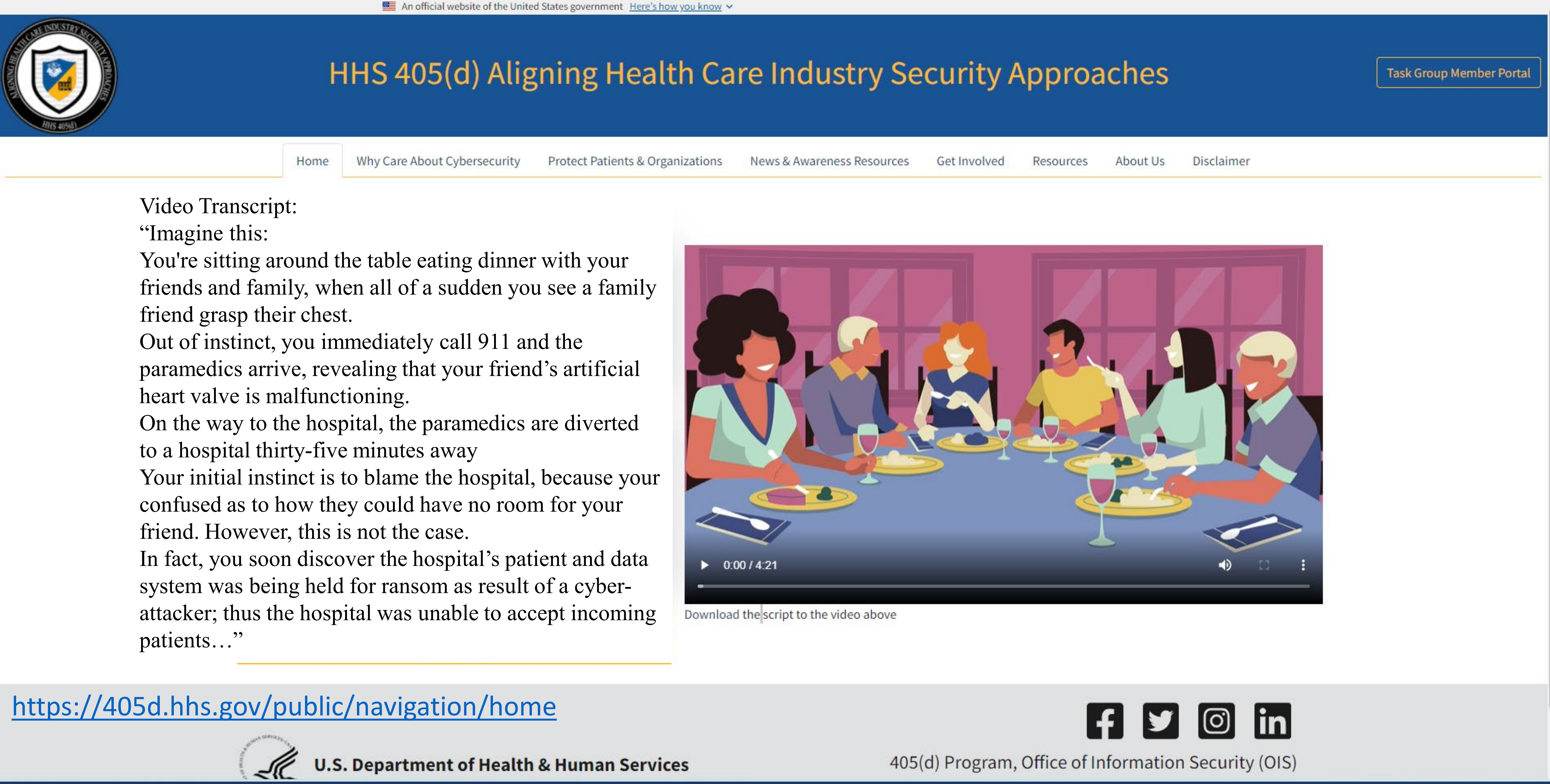
This publication is available free of charge from
https://doi.org/10.6028/NIST.SP.1800-30

The second draft of this publication is available free of charge from:
https://www.nccoe.nist.gov/sites/default/files/legacy-files/rpm-nist-sp1800-30-2nd-draft.pdf

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-30.pdf


An official website of the United States government Here's how you know
Task Group Member Portal
Home
Why Care About Cybersecurity
Protect Patients & Organizations
News & Awareness Resources
Get Involved
Resources
About Us
Disclaimer
0:00 / 4:21
U.S. Department of Health & Human Services

HHS 405(d) Aligning Health Care Industry Security Approaches

Video Transcript:
"Imagine this:
You're sitting around the table eating dinner with your friends and family, when all of a sudden you see a family friend grasp their chest.
Out of instinct, you immediately call 911 and the paramedics arrive, revealing that your friend's artificial heart valve is malfunctioning.
On the way to the hospital, the paramedics are diverted to a hospital thirty-five minutes away
Your initial instinct is to blame the hospital, because your confused as to how they could have no room for your friend. However, this is not the case.
In fact, you soon discover the hospital's patient and data system was being held for ransom as result of a cyber-attacker; thus the hospital was unable to accept incoming patients…"

Download the script to the video above

https://405d.hhs.gov/public/navigation/home

405(d) Program, Office of Information Security (OIS)

WEBINARS

NCTRC Webinar – Ransomware In Health

BY SOUTHWEST TELEHEALTH RESOURCE CENTER • OCTOBER 14, 2021

Ransomware in Health

TRC NATIONAL CONSORTIUM OF TELEHEALTH RESOURCE CENTERS

Ransomware in Health

October 14, 2021

Hosted by: Southwest Telehealth Resource Center

Outcome Objectives:
• Describe the basics of ransomware and why it poses cybersecurity and other risks.
• Determine weaknesses in healthcare systems. • Identify methods to counteract ransomware in medical settings.

Speakers:
-Jeanne E. Varner Powell, JD, Senior Legal Risk Management Consultant, MICA
-David Shelley, President, BVA Inc.

Moderator: Michael J Holcomb, Associate Director, Information Technology, Southwest Telehealth Resource Center, Arizona Telemedicine Program

https://telehealthresourcecenter.org/resources/webinars/nctrc-webinar-ransomware-in-health/

Health Information Privacy and Cybersecurity Resources

- BigID Blog: What Steps Should You Take For HIPAA Compliance? (What Are the Three Rules of HIPAA?)
- Collecting, Using, or Sharing Consumer Health Information? Look to HIPAA, the FTC Act, and the Health Breach Notification Rule
- Federal Trade Commission: Children's Privacy
- Federal Trade Commission: Health Privacy
- Halock: The Hand Rule: Managing the Upper Limits of Security Costs
- Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients
- HHS 405(d) Program: Aligning Health Care Industry Security Approaches: Cyber Safety is Patient Safety
- International Association of Privacy Professionals: US State Privacy Legislation Tracker
- NIST Cybersecurity Framework 2.0: RESOURCE & OVERVIEW GUIDE (NIST.SP.1299.pdf)
- Telehealth.HHS.gov: HIPAA Rules for telehealth technology
- Telehealth.HHS.gov: How do I protect my data and privacy?
- Telehealth.HHS.gov: Telehealth for behavioral health care: Protecting patients' privacy
- Telehealth.HHS.gov: Telehealth Privacy Tips for Patients
- Telehealth.HHS.gov: Telehealth Privacy Tips for Providers
- The HIPAA Journal: Security Breaches in Healthcare in 2023
- The NIST Cybersecurity Framework (CSF) 2.0 (NIST.CSWP.29.pdf)
- The Office of the National Coordinator for Health Information Technology: Guide to Privacy and Security of Electronic Health Information
- U.S. Department of Health and Human Services Office for Civil Rights Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information
- U.S. Department of Health and Human Services: Health Information Privacy
- U.S. Department of Health and Human Services: HIPAA and Telehealth: Telehealth Privacy and Security
- U.S. Department of Health and Human Services: Resource for Health Care Providers on Educating Patients about Privacy and Security Risks to Protected Health Information when Using Remote Communication Technologies for Telehealth
- U.S. Department of Health and Human Services: Summary of the HIPAA Privacy Rule
- U.S. Department of Health and Human Services: Summary of the HIPAA Security Rule
- U.S. Department of Health and Human Services: Telehealth Privacy and Security Tips for Patients
- Verizon: 2023 Data Breach Investigations Report Healthcare Snapshot
- Virtual Care Security Tips for patients
- Virtual Care Security Tips for providers

TELEHEALTH SECURITY AND PRIVACY TIPS FOR PROVIDERS

While telehealth provides a host of benefits for patient care, it also exposes healthcare delivery organizations (HDOs) to significant cyber risks. Here are some tips for improving the security and privacy of telehealth services for HDOs:

SHARE UPDATED PRIVACY AND SECURITY PRACTICES WITH YOUR PATIENTS. Communicating privacy and security practices with your patients should be an integral part of your overall patient engagement strategy.

USE HIPAA-COMPLIANT APPLICATIONS to provide telehealth services when practical, and limit the number of applications used to help reduce security and privacy risks.

ENABLE ALL AVAILABLE ENCRYPTION AND PRIVACY MODES when using third-party applications for telehealth services.

MANAGE MOBILE DEVICE ACCESS. Isolate personal mobile devices from HDO applications, networks, and patient data. Corporate-owned devices should be granted the most access to HDO networks and information while personal mobile devices should have the least.

LIMIT NETWORK ACCESS. Apply defense in depth, network segmentation, and the principle of least privilege to prevent unauthorized access to patient information and medical devices.

USE MULTIFACTOR AUTHENTICATION WHENEVER POSSIBLE, especially when it comes to accessing your organization's most sensitive data.

MAINTAIN GOOD CYBER HYGIENE. Healthy habits for your information technology systems and applications will go a long way toward keeping them safe and secure. Run updates for equipment and applications as soon as they are available to take advantage of the latest security capabilities.

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST CYBER

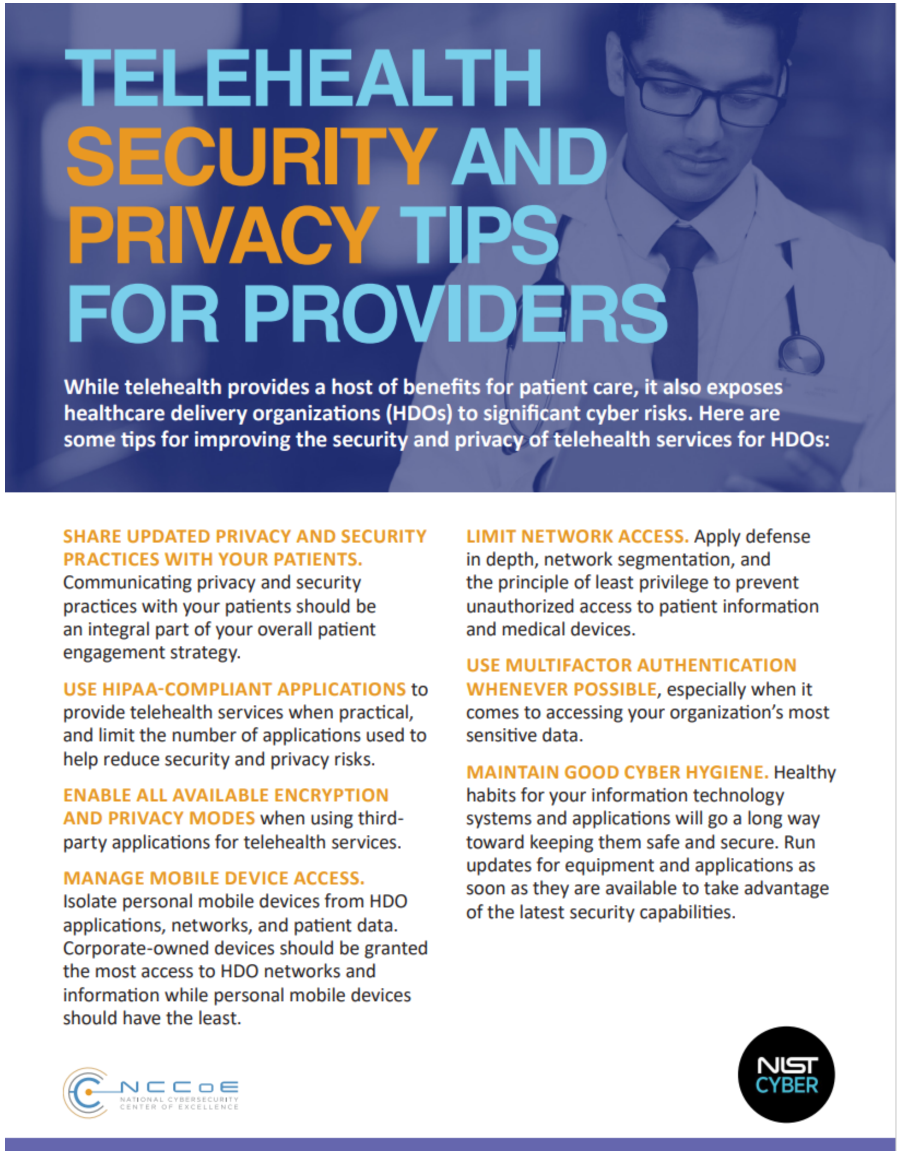
- **SHARE UPDATED PRIVACY AND SECURITY PRACTICES WITH YOUR PATIENTS**. Communicating privacy and security practices with your patients should be an integral part of your overall patient engagement strategy.

- **USE HIPAA-COMPLIANT APPLICATIONS** to provide telehealth services when practical, and limit the number of applications used to help reduce security and privacy risks.

- **ENABLE ALL AVAILABLE ENCRYPTION AND PRIVACY MODES** when using third party applications for telehealth services.

- **MANAGE MOBILE DEVICE ACCESS**. Isolate personal mobile devices from HDO applications, networks, and patient data. Corporate-owned devices should be granted the most access to HDO networks and information while personal mobile devices should have the least.

https://www.nccoe.nist.gov/sites/default/files/legacy-files/brochure-telehealth-hdo-tips.pdf



TELEHEALTH SECURITY AND PRIVACY TIPS FOR PROVIDERS

While telehealth provides a host of benefits for patient care, it also exposes healthcare delivery organizations (HDOs) to significant cyber risks. Here are some tips for improving the security and privacy of telehealth services for HDOs:

SHARE UPDATED PRIVACY AND SECURITY PRACTICES WITH YOUR PATIENTS. Communicating privacy and security practices with your patients should be an integral part of your overall patient engagement strategy.

USE HIPAA-COMPLIANT APPLICATIONS to provide telehealth services when practical, and limit the number of applications used to help reduce security and privacy risks.

ENABLE ALL AVAILABLE ENCRYPTION AND PRIVACY MODES when using third-party applications for telehealth services.

MANAGE MOBILE DEVICE ACCESS. Isolate personal mobile devices from HDO applications, networks, and patient data. Corporate-owned devices should be granted the most access to HDO networks and information while personal mobile devices should have the least.

LIMIT NETWORK ACCESS. Apply defense in depth, network segmentation, and the principle of least privilege to prevent unauthorized access to patient information and medical devices.

USE MULTIFACTOR AUTHENTICATION WHENEVER POSSIBLE, especially when it comes to accessing your organization's most sensitive data.

MAINTAIN GOOD CYBER HYGIENE. Healthy habits for your information technology systems and applications will go a long way toward keeping them safe and secure. Run updates for equipment and applications as soon as they are available to take advantage of the latest security capabilities.

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

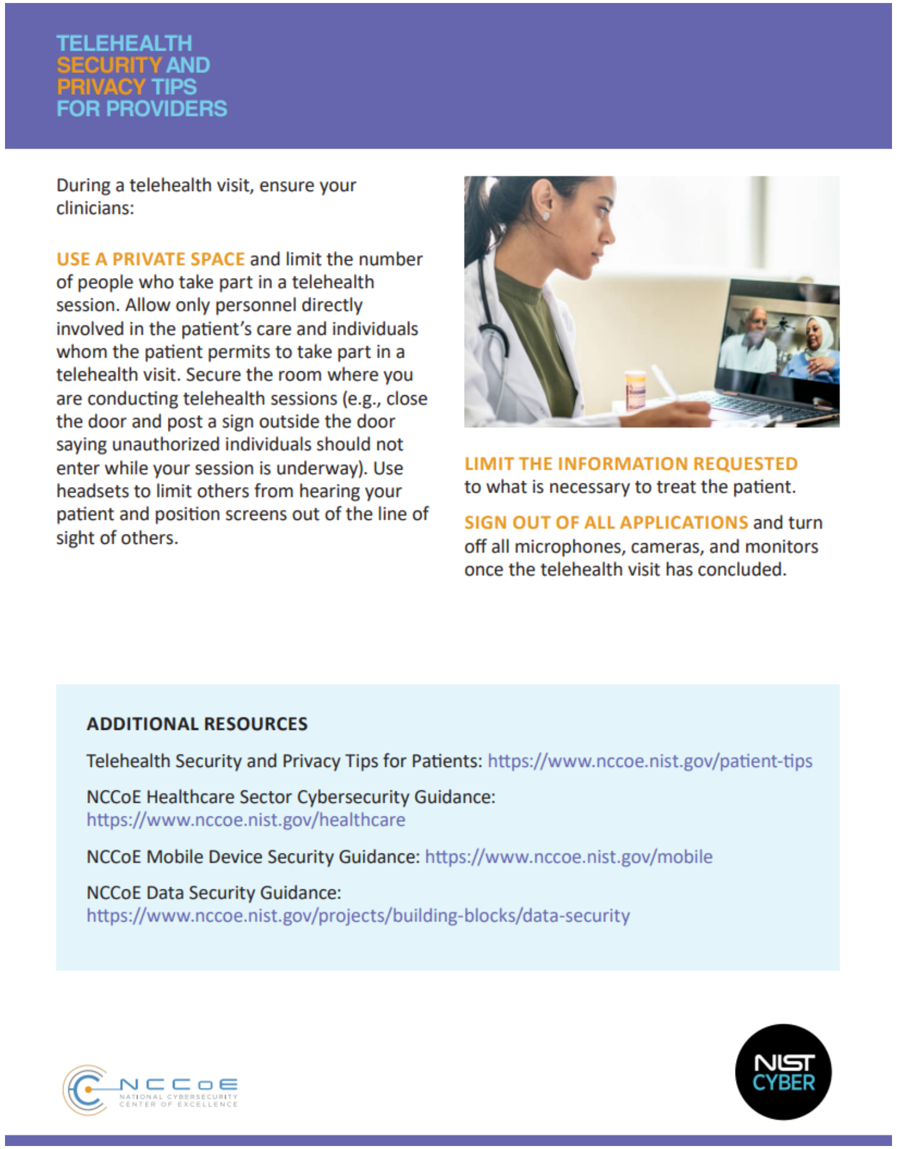
NIST CYBER

- **LIMIT NETWORK ACCESS**. Apply defense in depth, network segmentation, and the principle of least privilege to prevent unauthorized access to patient information and medical devices.

- **USE MULTIFACTOR AUTHENTICATION WHENEVER POSSIBLE**, especially when it comes to accessing your organization's most sensitive data.

- **MAINTAIN GOOD CYBER HYGIENE**. Healthy habits for your information technology systems and applications will go a long way toward keeping them safe and secure. Run updates for equipment and applications as soon as they are available to take advantage of the latest security capabilities.

https://www.nccoe.nist.gov/sites/default/files/legacy-files/brochure-telehealth-hdo-tips.pdf



TELEHEALTH SECURITY AND PRIVACY TIPS FOR PROVIDERS

During a telehealth visit, ensure your clinicians:

USE A PRIVATE SPACE and limit the number of people who take part in a telehealth session. Allow only personnel directly involved in the patient's care and individuals whom the patient permits to take part in a telehealth visit. Secure the room where you are conducting telehealth sessions (e.g., close the door and post a sign outside the door saying unauthorized individuals should not enter while your session is underway). Use headsets to limit others from hearing your patient and position screens out of the line of sight of others.

LIMIT THE INFORMATION REQUESTED to what is necessary to treat the patient.

SIGN OUT OF ALL APPLICATIONS and turn off all microphones, cameras, and monitors once the telehealth visit has concluded.

ADDITIONAL RESOURCES

Telehealth Security and Privacy Tips for Patients: https://www.nccoe.nist.gov/patient-tips

NCCoE Healthcare Sector Cybersecurity Guidance: https://www.nccoe.nist.gov/healthcare

NCCoE Mobile Device Security Guidance: https://www.nccoe.nist.gov/mobile

NCCoE Data Security Guidance: https://www.nccoe.nist.gov/projects/building-blocks/data-security

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

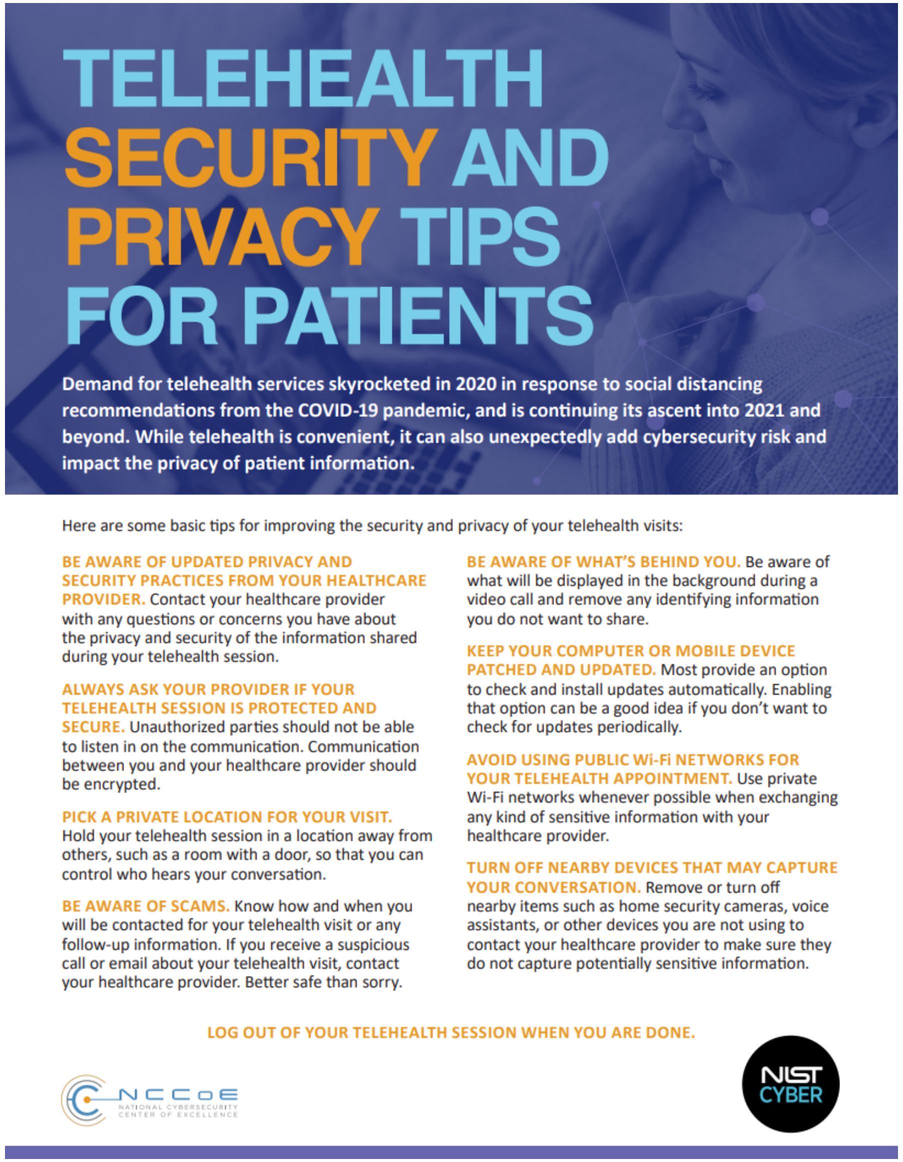
NIST CYBER

- **USE A PRIVATE SPACE** and limit the number of people who take part in a telehealth session. Allow only personnel directly involved in the patient's care and individuals whom the patient permits to take part in a telehealth visit. Secure the room where you are conducting telehealth sessions (e.g., close the door and post a sign outside the door saying unauthorized individuals should not enter while your session is underway). Use headsets to limit others from hearing your patient and position screens out of the line of sight of others.

- **LIMIT THE INFORMATION REQUESTED** to what is necessary to treat the patient.

- **SIGN OUT OF ALL APPLICATIONS** and turn off all microphones, cameras, and monitors once the telehealth visit has concluded

https://www.nccoe.nist.gov/sites/default/files/legacy-files/brochure-telehealth-hdo-tips.pdf



TELEHEALTH SECURITY AND PRIVACY TIPS FOR PATIENTS

Demand for telehealth services skyrocketed in 2020 in response to social distancing recommendations from the COVID-19 pandemic, and is continuing its ascent into 2021 and beyond. While telehealth is convenient, it can also unexpectedly add cybersecurity risk and impact the privacy of patient information.

Here are some basic tips for improving the security and privacy of your telehealth visits:

BE AWARE OF UPDATED PRIVACY AND SECURITY PRACTICES FROM YOUR HEALTHCARE PROVIDER. Contact your healthcare provider with any questions or concerns you have about the privacy and security of the information shared during your telehealth session.

ALWAYS ASK YOUR PROVIDER IF YOUR TELEHEALTH SESSION IS PROTECTED AND SECURE. Unauthorized parties should not be able to listen in on the communication. Communication between you and your healthcare provider should be encrypted.

PICK A PRIVATE LOCATION FOR YOUR VISIT. Hold your telehealth session in a location away from others, such as a room with a door, so that you can control who hears your conversation.

BE AWARE OF SCAMS. Know how and when you will be contacted for your telehealth visit or any follow-up information. If you receive a suspicious call or email about your telehealth visit, contact your healthcare provider. Better safe than sorry.

BE AWARE OF WHAT'S BEHIND YOU. Be aware of what will be displayed in the background during a video call and remove any identifying information you do not want to share.

KEEP YOUR COMPUTER OR MOBILE DEVICE PATCHED AND UPDATED. Most provide an option to check and install updates automatically. Enabling that option can be a good idea if you don't want to check for updates periodically.

AVOID USING PUBLIC Wi-Fi NETWORKS FOR YOUR TELEHEALTH APPOINTMENT. Use private Wi-Fi networks whenever possible when exchanging any kind of sensitive information with your healthcare provider.

TURN OFF NEARBY DEVICES THAT MAY CAPTURE YOUR CONVERSATION. Remove or turn off nearby items such as home security cameras, voice assistants, or other devices you are not using to contact your healthcare provider to make sure they do not capture potentially sensitive information.

LOG OUT OF YOUR TELEHEALTH SESSION WHEN YOU ARE DONE.

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST CYBER

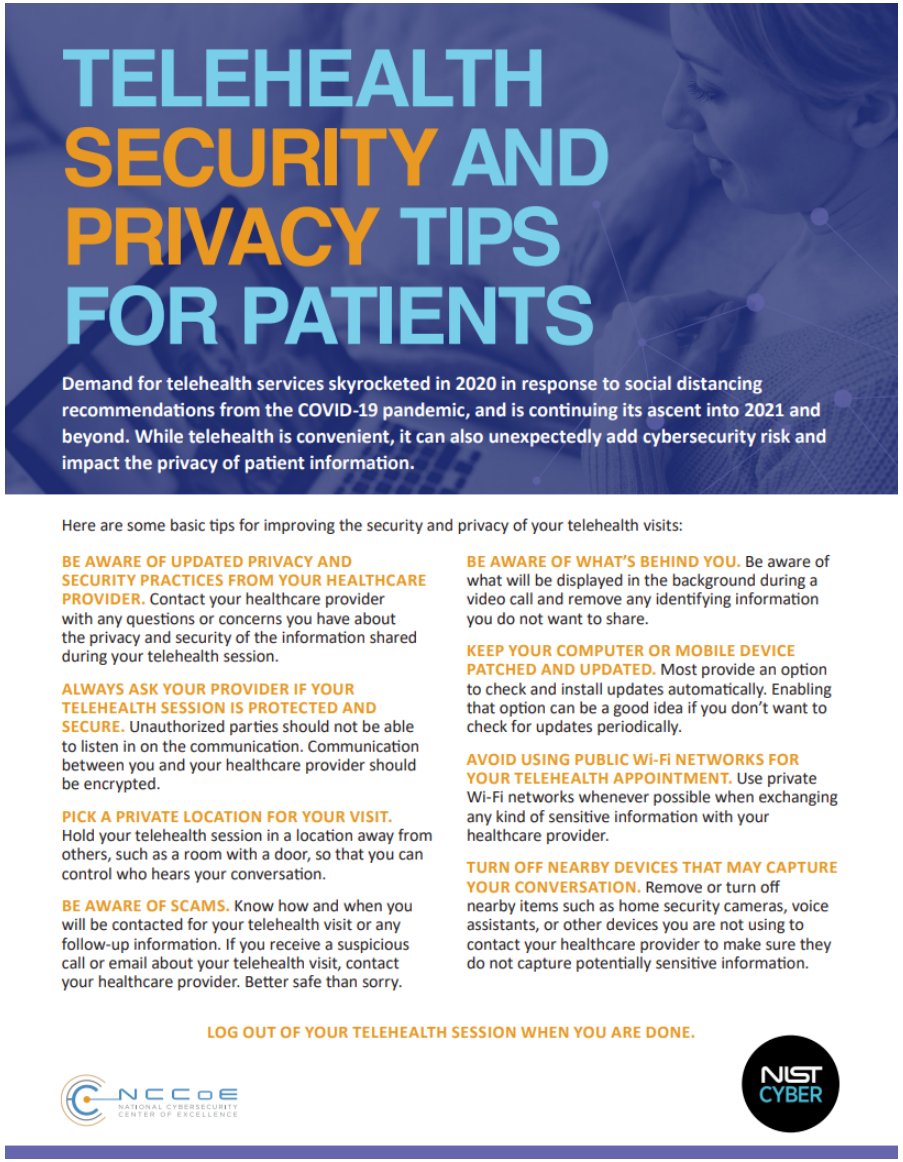
- **BE AWARE OF UPDATED PRIVACY AND SECURITY PRACTICES FROM YOUR HEALTHCARE PROVIDER**. Contact your healthcare provider with any questions or concerns you have about the privacy and security of the information shared during your telehealth session.

- **ALWAYS ASK YOUR PROVIDER IF YOUR TELEHEALTH SESSION IS PROTECTED AND SECURE**. Unauthorized parties should not be able to listen in on the communication. Communication between you and your healthcare provider should be encrypted.

- **PICK A PRIVATE LOCATION FOR YOUR VISIT**. Hold your telehealth session in a location away from others, such as a room with a door, so that you can control who hears your conversation.

- **BE AWARE OF SCAMS**. Know how and when you will be contacted for your telehealth visit or any follow-up information. If you receive a suspicious call or email about your telehealth visit, contact your healthcare provider. Better safe than sorry.

https://www.nccoe.nist.gov/sites/default/files/legacy-files/brochure-telehealth-patient-tips.pdf



TELEHEALTH SECURITY AND PRIVACY TIPS FOR PATIENTS

Demand for telehealth services skyrocketed in 2020 in response to social distancing recommendations from the COVID-19 pandemic, and is continuing its ascent into 2021 and beyond. While telehealth is convenient, it can also unexpectedly add cybersecurity risk and impact the privacy of patient information.

Here are some basic tips for improving the security and privacy of your telehealth visits:

BE AWARE OF UPDATED PRIVACY AND SECURITY PRACTICES FROM YOUR HEALTHCARE PROVIDER. Contact your healthcare provider with any questions or concerns you have about the privacy and security of the information shared during your telehealth session.

ALWAYS ASK YOUR PROVIDER IF YOUR TELEHEALTH SESSION IS PROTECTED AND SECURE. Unauthorized parties should not be able to listen in on the communication. Communication between you and your healthcare provider should be encrypted.

PICK A PRIVATE LOCATION FOR YOUR VISIT. Hold your telehealth session in a location away from others, such as a room with a door, so that you can control who hears your conversation.

BE AWARE OF SCAMS. Know how and when you will be contacted for your telehealth visit or any follow-up information. If you receive a suspicious call or email about your telehealth visit, contact your healthcare provider. Better safe than sorry.

BE AWARE OF WHAT'S BEHIND YOU. Be aware of what will be displayed in the background during a video call and remove any identifying information you do not want to share.

KEEP YOUR COMPUTER OR MOBILE DEVICE PATCHED AND UPDATED. Most provide an option to check and install updates automatically. Enabling that option can be a good idea if you don't want to check for updates periodically.

AVOID USING PUBLIC Wi-Fi NETWORKS FOR YOUR TELEHEALTH APPOINTMENT. Use private Wi-Fi networks whenever possible when exchanging any kind of sensitive information with your healthcare provider.

TURN OFF NEARBY DEVICES THAT MAY CAPTURE YOUR CONVERSATION. Remove or turn off nearby items such as home security cameras, voice assistants, or other devices you are not using to contact your healthcare provider to make sure they do not capture potentially sensitive information.

LOG OUT OF YOUR TELEHEALTH SESSION WHEN YOU ARE DONE.

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST CYBER

- **BE AWARE OF WHAT'S BEHIND YOU**. Be aware of what will be displayed in the background during a video call and remove any identifying information you do not want to share.

- **KEEP YOUR COMPUTER OR MOBILE DEVICE PATCHED AND UPDATED**. Most provide an option to check and install updates automatically. Enabling that option can be a good idea if you don't want to check for updates periodically.

- **AVOID USING PUBLIC Wi-Fi NETWORKS FOR YOUR TELEHEALTH APPOINTMENT**. Use private Wi-Fi networks whenever possible when exchanging any kind of sensitive information with your healthcare provider.

- **TURN OFF NEARBY DEVICES THAT MAY CAPTURE YOUR CONVERSATION**. Remove or turn off nearby items such as home security cameras, voice assistants, or other devices you are not using to contact your healthcare provider to make sure they do not capture potentially sensitive information.

https://www.nccoe.nist.gov/sites/default/files/legacy-files/brochure-telehealth-patient-tips.pdf

Healthcare & Public Health Sector Coordinating Councils

PUBLIC PRIVATE PARTNERSHIP

HEALTH INDUSTRY CYBERSECURITY - SECURING TELEHEALTH AND TELEMEDICINE

April 2021

The Health Sector Coordinating Council (HSCC) has developed this white paper, the “Health Industry Cybersecurity – Securing Telehealth and Telemedicine (HIC-STAT)” guide,- for the benefit of health care systems, clinicians, vendors and service providers, and patients. All of these stakeholders share responsibility for ensuring that telehealth services achieve their optimum benefit with minimal risk to the privacy and security of the data, the consultations, and the systems hosting them.

https://www.aha.org/guidesreports/2021-04-20-healthcare-and-public-health-sector-coordinating-councils-public-private

Arizona Telemedicine Program

Southwest TRC Telehealth Resource Center™

Thank you!

Questions?

mholcomb@telemedicine.arizona.edu