

**Helping Healthcare Providers Adopt
Digital Health Technologies and Achieve
HIE Connectivity in the District**

Digital Health Technical Assistance Program Learning Community

Security Awareness & Privacy





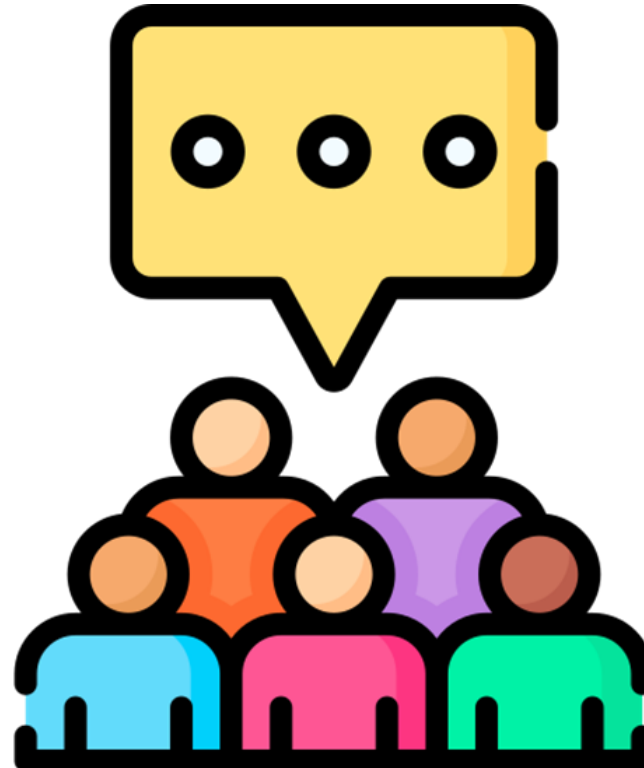
Jennifer Moore
Zane Networks



Rocio Payne
Clinovations



The eHealthDC **EHR Data Quality Technical Assistance** learning communities are designed to promote knowledge sharing amongst participants and will require ongoing interaction and active participation among attendees.





- Use **Chat** to share questions and comments with the group



- Use **Raise Hand** function for questions or comments to share with the group



- **Cameras on** are encouraged for a more interactive and engaging experience





Our Vision: A future where high-quality data is captured, shared, and used to drive coordinated, efficient, whole-person care.

Our Mission: To deliver integrated, tailored EHR and HIE technical assistance that equips providers with the knowledge, skills and confidence to capture accurate, high-quality data, enable seamless and secure exchange, and use information to improve care delivery.

New Digital Health TA Program Opportunity

Free Technical Assistance available to improve EHR data quality, strengthen data exchange with CRISP DC and integrate HIE tools into daily workflows.



eHEALTHDC
A DISTRICT OF COLUMBIA PRIMARY CARE ASSOCIATION PROGRAM
Digital Health Technical Assistance Collaborative

Program Overview
eHealthDC is the District's Digital Health Technical Assistance Collaborative, made up of regional health leaders including the DC Primary Care Association (DCPCA), Clinovations, CRISP DC, DC Hospital Association (DCHA) and Zane Networks.

Funded by the DC Department of Health Care Finance (DHCF), our team of eHealthDC experts provides free, tailored technical assistance support to ambulatory organizations and hospitals to help improve EHR data quality, boost interoperability, and integrate CRISP DC HIE tools into daily workflows.

Technical Support & Assistance Pathways

 EHR Data Quality and Workflow Optimization	 Health Information Exchange Adoption
<ul style="list-style-type: none">• Standardize Data Capture: Optimize structured EHR data entry for consistent documentation• Optimize Workflows: Use workflow mapping to identify and bridge critical gaps• Strengthen Quality Reporting: Support clinical documentation improvement and performance metrics for accurate reporting	<ul style="list-style-type: none">• Expand HIE Awareness & Use: Provide CRISP DC onboarding support and tool training• Enhance Care Coordination: Integrate HIE data into clinical workflows to improve decision-making• Improve Population Health: Use HIE tools to drive readiness for value-based care

Why This Matters
By aligning EHR data quality and health information exchange, this technical assistance supports more coordinated care, stronger data for reporting, and progress toward whole-person and value-based care models

DHCF

Click here to take our brief survey to receive free, tailored technical assistance. An eHealthDC team member will follow up on next steps
Questions? Email: contact@e-healthdc.org



Complete the [Interest Form](#) or reach out to contact@e-healthdc.org and we'll be in touch!



1

Provide basic, high-level knowledge of the most common types of cybersecurity threats — including new AI-powered attacks

2

Bring attention to habits and behaviors we all can employ to minimize the risk of cyberattacks and better protect sensitive patient data in your EHR

3

Review HIPAA regulatory requirements — Privacy Rule, Security Rule, and Breach Notification Rule — to maintain compliance with Federal mandates

4

Provide practical tools, tips and resources to help your organization build a culture of security

Cyber Attack

What is a cyber attack?

“A cyberattack is any intentional effort to steal, expose, alter, disable, or destroy data, applications, or other assets through unauthorized access to a network, computer system or digital device” - IBM

Failed

Cyber Incidents Hitting Close to Home: DC/MD/VA

MedStar Health (2016)

~\$1M+ Recovery

Ransomware shut down 10 DC-area hospitals. MedStar refused to pay ransom; recovery costs exceeded \$1M with weeks of paper-based operations.

Prince George's County Health Dept. (2023)

Cost Undisclosed

Phishing attack exposed ~50K patient records including SSNs. Financial remediation costs not publicly disclosed; breach notification and credit monitoring added significant expense.

Inova Health System, VA (2020)

\$3.9M Settlement

Third-party vendor breach exposed 1.5M Northern Virginia patients' records. Inova settled a class-action lawsuit for \$3.9M — a reminder that vendor risk is your risk.

DC Health Link (2023)

\$6M+ Response Cost

Breach exposed data of Congress members and staff, triggering Senate hearings. DC Health Benefit Exchange Authority spent \$6M+ on investigation, remediation, and credit monitoring.

Impact and Consequences of a Cyberattack

Direct Patient Care	Practice Impact	Patients & Employees
<ul style="list-style-type: none">• Medical devices stop working or are corrupted• EHR records — prescriptions, diagnoses — become inaccessible or lost• Forced to use temporary paper systems causing delays and errors• Payment systems go down	<ul style="list-style-type: none">• Ransom payments, lawsuits, system recovery costs• Regulatory penalties• Damaged reputation• Lost patient trust• Recovery takes 100+ days on average	<ul style="list-style-type: none">• Identity theft — SSN, DOB, and address used to open fraudulent accounts• Fraud affects families, friends, and coworkers• Strained employee morale and burnout

How do malicious actors break into your systems?

Phishing

Phishing is a cybercrime in which a target is contacted by email, phone, or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking details, or passwords.

The information is then used to access important accounts and can result in identity theft and financial loss.

85% of breaches start with phishing (HHS)

Attack Channels:



Email



Phone Call (Vishing)



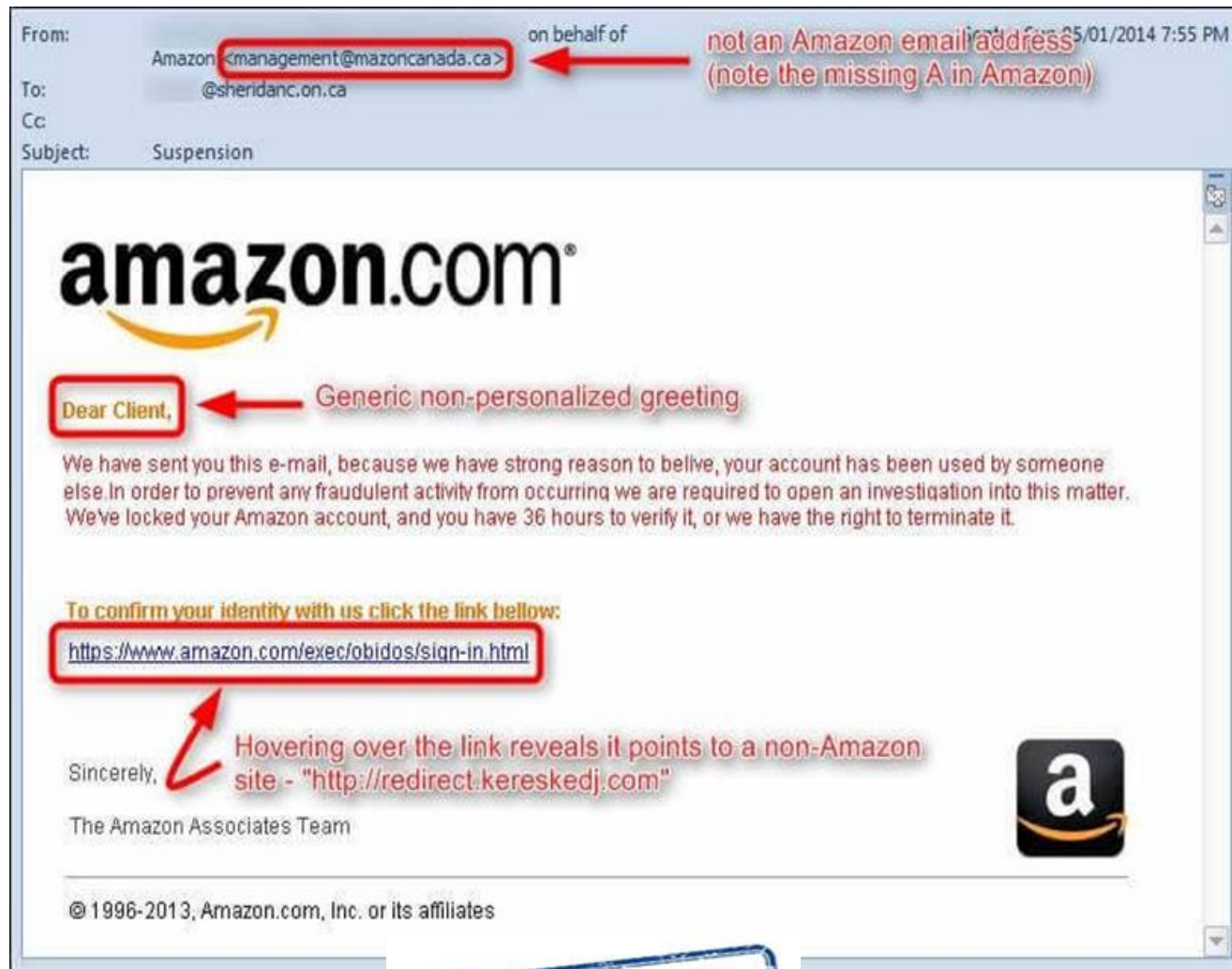
Texting (SMiShing)



QR Code (Quishing)

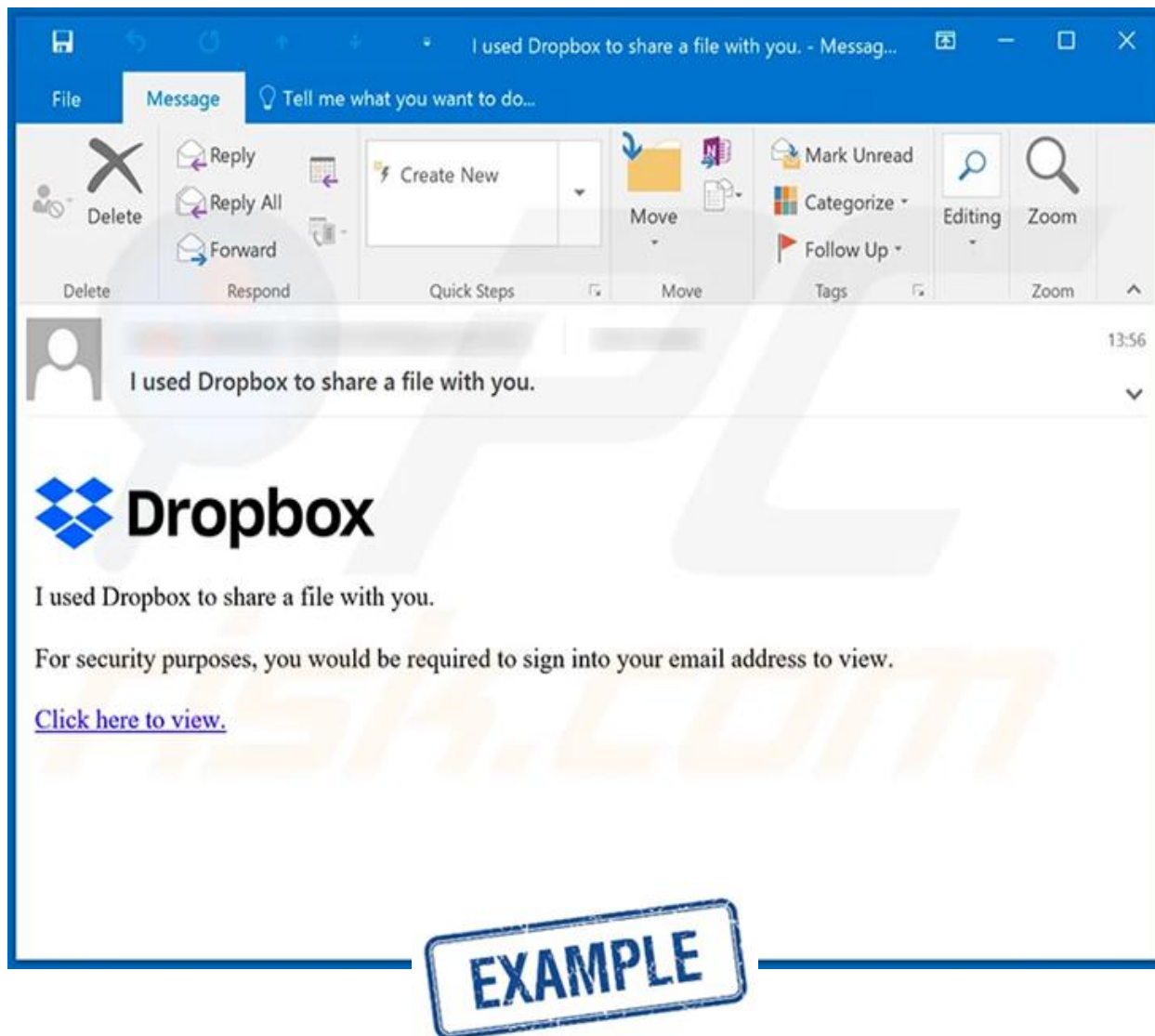


MFA Fatigue (MFA Bombing)

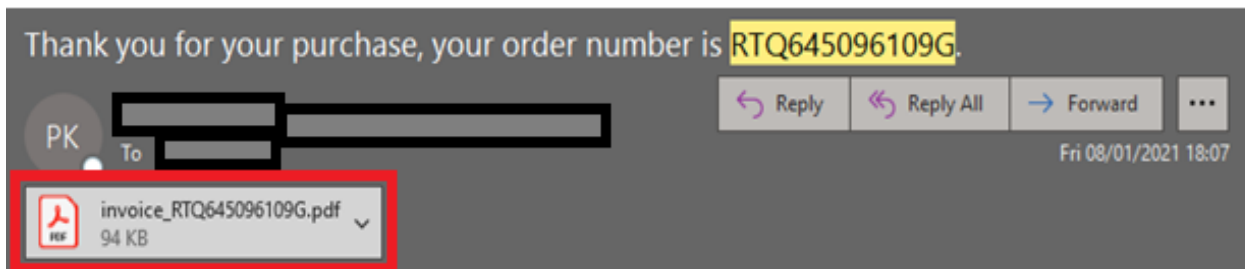


EXAMPLE

- Appears to be from well-known Company like Amazon asking you to sign-in and **urgently** correct an issue with your account
- **Links** point to a website pretending to be from the company's legitimate site and asks to log in
- **TIP: DO NOT CLICK** on any links in the email – If in doubt, directly log-in to your account by typing the company address directly into your web browser.



- Contains a **link** to what appears to be a shared file on OneDrive, Google Docs, Dropbox or any other file sharing site
- Link points to a website pretending to be from a file sharing site and requests you to log in
- **TIP: DO NOT CLICK** any links in the email instead login to your account and find the file shared by name – Remember to verify sender's identity



EXTERNAL

Dear customer,
We have passed your order #RTQ645096109G to the distribution facility.

In the invoice you can find all the information about your charge.
To learn more about the complete cost and data about charging and delivery tap the receipt attached to this letter.

Your order will be send to you in a shortest time, our managers already working on it!

You will be notified when your order will be ready for sending.

Before the delivery process, the messenger will reach out to you.

We have faith you enjoy your purchase!

Please contact us here if you would like to modify / cancel the order:1 (831) 400 5370

Thank you for choosing us.

Regards online store Rose Delivery

EXAMPLE

- Contains an **attachment** presented as an unpaid invoice and claims service will be terminated if invoice is not paid in full
- Targets individuals (by pretending to be a retailer) or business (by impersonating a vendor or a supplier)
- **TIP: DO NOT DOWNLOAD THE ATTACHMENT.** Contact the vendor/service directly using official contact information before submitting payment



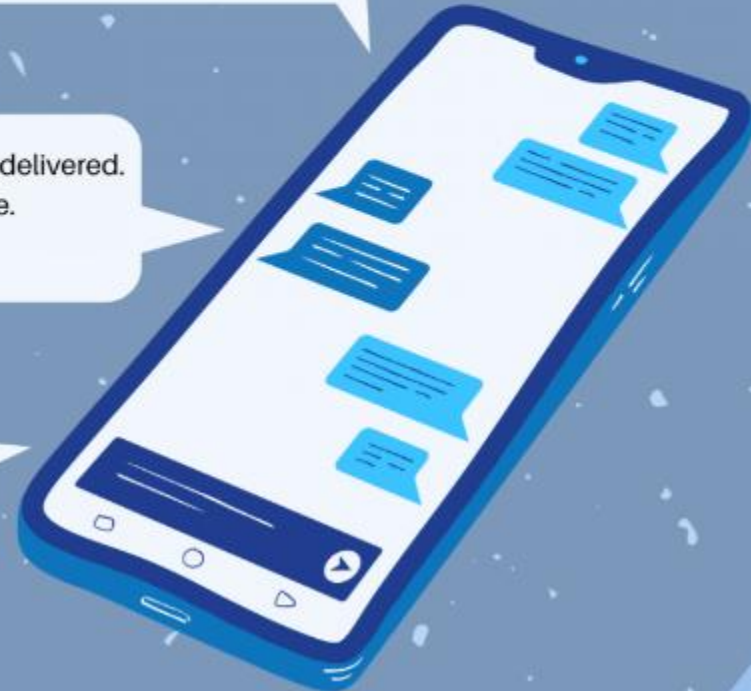
Smishing



You're a WINNER!! Follow the link to claim your \$1,000 Amazon giftcard!
www.freeamzgiftcrd.com

Your Fedex package could not be delivered. Follow the link to resolve this issue.
<http://FEDX.Suprt/c2s8yjgh8>

⚠ Alert! We have detected fraudulent activity on your BOA account. To resolve this issue click here.
<https://Alrt.boa/secu>



Can you identify the signs of a phishing email?



From: Helpdesk <helpdesk-infotech@gmail.com>

To:

Subject: Fraud Alert!

Attachment: Password Reset Details.exe

Dear Info-Tech user,

We have recently detected a login to your online account that was not performed by you. In order to rectify this situation please go to InfoTech website [here](#) to change your password to ensure your account is secure. The documnt attached will guide you through the reset process. If you are unable to reset your password on the website please send me your account details and I will verify your account for you. If you fail to do so by next week will result in your account being deleted.

Sincerely,

Info Tech

EXAMPLE



From: Helpdesk <helpdesk-infotech@gmail.com>

1

To:

Subject: Fraud Alert!

2

Attachment: Password Reset Details.exe

3

Dear Info-Tech user,

4

We have recently detected a login 5 our online account that was not 6 rmed by you. In order to rectify this situation please go to InfoTech website here to change your password to ensure your account is secure. The 7 document attached will guide you through the reset process. If you are unable to reset your password on the website please send me your account details 8 I will verify your account for you. If you fail to 9 by next week will result in your account being deleted.

10

Sincerely,

Info Tech

11

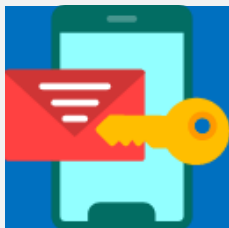
EXAMPLE

New Phishing Tactics: MFA (Multi-Factor Authentication) Fatigue & QR Code Phishing

MFA Fatigue Attack — "New Concept"

How it works:

Attacker triggers repeated MFA push notifications to your phone using stolen credentials. Victim taps Approve out of frustration to stop the notifications — granting the attacker full access.



TIP:

NEVER APPROVE an MFA request you did not initiate. Deny all unexpected prompts and report to IT Security immediately.

QR Code Phishing ("Quishing") — "New Concept"

How it works:

Attacker emails a QR code image — which bypasses standard email security filters because there's no suspicious link to scan. Scanning with your phone opens a fake login page outside corporate security controls.



TIP:

Do NOT scan QR codes in unexpected emails. Preview the URL first and verify with the sender through a separate channel.

HOW TO SPOT & STOP PHISHING

SPOT IT

- 1 Urgent or threatening language
- 2 Suspicious sender information
- 3 Out of the ordinary requests
- 4 Impersonal or generic greetings
- 5 Requests for personal information
- 6 Unusual formatting or suspicious layout

STOP IT

- **Be cautious with links & attachments**
Avoid clicking suspicious links or unknown attachments
- **Verify links before clicking**
Hover to check for https and correct spelling
- **Keep software updated**
Use up-to-date browsers and anti-phishing plug-ins
- **Never share personal info via email**
Avoid providing personal information through email
- **Confirm requests directly**
Contact the sender via a known, trusted method
- **Contact IT for verification**
When uncertain, reach out to your IT department



Social Engineering: Use of deception to manipulate well-meaning individuals into divulging confidential information or that person's personal information which may be used for fraudulent purposes.

With Artificial Intelligence (AI), attackers can now create a digital twin of your face and voice and use them to say and do anything they want.

Three seconds of your Youtube, Facebook or Tiktok video is sufficient to clone likeness.



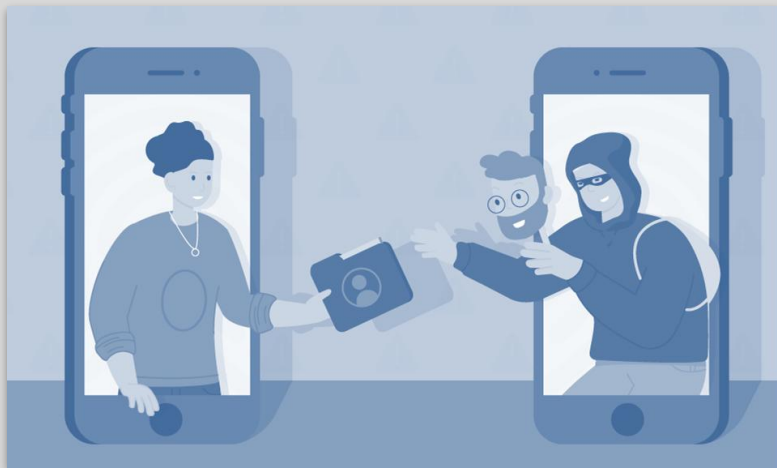
Original



Deepfake



PROTECT YOURSELF AGAINST SOCIAL ENGINEERING



- Don't perform any financial transactions, share passwords or personal information over the phone even if the voice sounds familiar.
- Never provide any confidential information when a representative unexpectedly calls you by phone. Ask to hang up and call back using a known number to verify the caller is legitimate.
- If the caller insists that you stay on the call, this is a red flag. Hang up immediately and alert your IT/security department.
- Minimize the amount of personal data on social media platforms. We often share our personal information indirectly on social media. However, malicious actors can use this information to conduct Brute Force attacks.

Protecting Your Passwords

According to HHS, 85% of cyber criminals accessed critical systems using stolen credentials

Convert a phrase to a strong password

"For the first time in forever" → 4da1stTymein4eva (Frozen)

Change default passwords

On routers, printers, and medical devices — defaults are publicly known

Avoid reusing the same password across accounts

One breach exposes every account with the same password

Use a password manager

Bitwarden (free), Keeper, or 1Password — generates and stores unique passwords

Enable MFA on every account

A second factor blocks 99% of automated attacks even with a stolen password

Two of the following passwords are considered strong passwords. Which two are they?

a)

ilovecats

b)

14A&A41

c)

iloveKatzs123

d)

!cedTisgr84\$umm3R

Two of the following passwords are considered strong passwords. Which two are they?

a)

ilovecats

b)

14A&A41

c)

iloveKatzs123

d)

!cedTisgr84\$umm3R



How To Protect Your Practice From Cyber Threats

Primary Purpose of HIPAA Regulations

The main objective of HIPAA is to uphold and protect the data integrity of Protected Health Information (PHI). It includes three rules:

HIPAA Privacy Rule

Creates standards for the privacy of PHI

- Applies to covered entities: providers, health plans, clearinghouses, and business associates
- PHI may only be used or disclosed as the Rule permits or with written patient authorization
- Requires a Notice of Privacy Practices (NPP) for patients
- Fosters trust and protects PHI from loss, theft, or misuse

HIPAA Security Rule

Standardizes handling of electronic PHI (ePHI)

- Requires administrative, physical, and technical safeguards
- Mandates regular risk assessments and staff training
- Covers every device that stores, accesses, or transmits ePHI — not just EHRs
- Applies to cloud-connected devices and medical IoT

Breach Notification Rule

Sets notification requirements after a breach

- Notify affected patients within 60 days of discovery
- Report to HHS Secretary via official breach form
- If 500+ records involved: notify local media as well
- Document: what PHI was involved, who accessed it, mitigation steps taken



HIPAA Privacy Rule: Safeguard Requirements

Use and Disclosure —

A covered entity may not use or disclose PHI, except: (1) as the Privacy Rule permits or requires, or (2) as the individual who is the subject of the information authorizes in writing.

Get Authorization —

Get written permission from the patient to use redacted ePHI for research, fundraising, or marketing.

Notice of Privacy Practices (NPP) —

An NPP is required to officially inform patients and subscribers of data-sharing policies.



Let's Discuss! Can you email patients? If so, what policies does your organization have in place when communicating with patients via email?



Can you email patients?

- The HIPAA Privacy Rule allows covered health care providers to communicate via email provided there are safeguards in place:
 - HIPAA Standard 164.312(d) requires providers to implement procedures to verify that persons or entities seeking access to ePHI are who they claim to be
 - HIPAA Standard 164.306(b) requires providers to implement reasonable and appropriate security measures

Should you email patients? It depends....

- Some organizations explicitly consent patients to acknowledge or opt out of email communications
- EHR patient portals offer secure messaging communications
- Regular emails are not encrypted and is not secure, sometimes households share email addresses
- If a patient emails you first, you can assume that email is acceptable
- Share only appropriate information via email



HIPAA Security Rule: Administrative Safeguards

Risk Management

A Security Risk Assessment is required and must be reassessed at regular intervals. A sanctions policy must be in place for non-compliance.

Comprehensive Policies & Procedures

Develop and consistently update cybersecurity policies aligned with best practices. These serve as the foundation for consistent information security.

Train Your Staff

Train employees on all ePHI access protocols and how to recognize phishing, hacking, social engineering, and AI-enabled threats. Keep training records.

Incident Response Readiness

Develop a robust IR plan detailing procedures for a security incident. Conduct regular drills — including AI threat scenarios (ransomware, deepfake).

Build Contingencies

Maintain ongoing business continuity with a preparation process that keeps data safe — including tested backup and disaster recovery plans.

HIPAA Security Rule: Technical Safeguards

Network Encryption

Encrypt any ePHI transmitted over external networks per NIST cryptographic standards. Includes device telemetry from cloud-connected medical devices.

Authenticate ePHI

Identify and authenticate ePHI; protect it from unauthorized changes and accidental destruction.

Control Activity Audits

Detailed logging is required to track all ePHI access attempts and monitor how ePHI is manipulated. Especially critical for AI tools that access patient data.

Encrypt Devices

All endpoint devices — including mobile phones, laptops, and tablets — must be able to encrypt and decrypt data.

Control Access

Each user must have a centrally-controlled unique username and PIN. Never share logins — shared credentials make auditing impossible.

Enable Automatic Logoff

Users must be logged out after 30 seconds to 3 minutes of inactivity depending on the application. Applies to all clinical workstations.

HIPAA Security Rule: Physical Safeguards

Control Facility Access

Track specific individuals who have physical access to data storage — engineers, repair people, and custodians. Take reasonable steps to block unauthorized entry.

Manage Workstations

Define which workstations can access health data. Specify how screens should be guarded from viewing at a distance. Use privacy screens in open areas.

Protect Mobile Devices

Implement a mobile device policy. Remove all data before a device is circulated to another user. Include medical devices and tablets.

Track Servers & Infrastructure

Maintain a complete inventory of all infrastructure with location information. Copy all data completely before moving servers.

ONC: Security Risk Assessment Tool (SRA)

HIPAA § 164.308(a)(1): A covered entity must "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the organization"

What to include in your SRA:

- ALL electronic devices that store, capture, or access ePHI — including EHR hardware/software, tablets, mobile phones, copiers, and printers
- Third-party vendor access — business associates must also comply; reviewing their security posture is your obligation
- **Cloud-connected medical devices and any AI tools that process patient data**

Free tool available:

- ONC/HHS Security Risk Assessment (SRA) Tool — free, wizard-based, designed for small and medium practices
- Available at: healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

Section 1: SRA Basics

Select the vulnerabilities that apply to your practice from the list below.

- ☒ Inadequate risk awareness or failure to identify new weaknesses
- ☒ Failure to remediate known risk(s)
- ☐ Failure to meet minimum regulatory requirements and security standards
- ☒ Inadequate Asset Tracking
- ☐ Unspecified workforce security responsibilities

Section 1: SRA Basics

Please rate the likelihood and impact on your practice of each potential threat.

	Likelihood			Impact		
	L	M	H	L	M	H
☒ Inadequate risk awareness or failure to identify new weaknesses						
Non-physical threat(s) such as data corruption or information disclosure, interruption of system function and business processes, and/or legislation or security breaches	L	M	H	L	M	H
Physical threats such as unauthorized facility access, hardware or equipment malfunction, collisions, trip/fire hazards, and/or hazardous materials (chemicals, magnets, etc.)	L	M	H	L	M	H
Natural threat(s) such as damage from dust/particulates, extreme temperatures, severe weather events, and/or destruction from animals/insects	L	M	H	L	M	H
Man-Made threat(s) such as insider carelessness, theft/vandalism, terrorism/civil unrest, toxic emissions, or hackers/computer criminals	L	M	H	L	M	H
Infrastructure threat(s) such as building/road hazards, power/telephone outages, water leakage (pipes, roof,	L	M	H	L	M	H

True or False?

My security risk assessment only needs to look at my EHR.

False! Review all electronic devices that store, capture, or modify electronic protected health information. Include your EHR hardware and software and devices that can access your EHR data (e.g., your tablet computer, your practice manager's mobile phone). Remember that copiers also store data.

True or False?

I have to outsource the security risk analysis assessment.

False! It is possible for small practices to do risk analysis themselves using self-help tools. However, doing a thorough and professional risk analysis that will stand up to a compliance review will require expert knowledge that could be obtained through services of an experienced outside professional.



What to do to minimize the impact of a breach

3 Phases of Backup and Recovery

Backup and recovery plans help maintain HIPAA compliance and minimize the impact of a data breach.

1 Assess

- Map all data: EHR, billing, scheduling, and clinical records
- Where is data stored? How much? How fast is it growing?
- Who is impacted if unavailable? How long can you manage?
- What can you afford to lose? What is your recovery window?

2 Implement

- Weekly full backup + nightly differential backups (minimum)
- All backups encrypted and stored securely — use 3-2-1 rule: 3 copies, 2 media, 1 offsite/offline
- Document: Incident Response Plan, Disaster Recovery Plan, Business Continuity Plan

3 Review

- Quarterly: restore test files to verify backup integrity
- Annually: revisit all policies and procedures for relevance
- If cloud/SaaS EHR: ask vendor for their backup SLA, RTO (recovery time), and RPO (recovery point) in writing

Your Cybersecurity Toolkit

Risk Assessment

- [ONC Security Risk Assessment Tool](#) (free — healthit.gov)
- [Posture](#) (commercial SRA tool and advisory services)

Breach & Response

- [HHS Breach Notification submission portal](#)



Cyber Safety Trainings/Resources

- [Cyber Safety Knowledge on Demand](#)
- [Cyber Safety Resource Library](#)

Password Managers

- [Keeper Security](#)
- [Bitwarden](#) (free trial available)
- [1Password](#)

Questions?

Upcoming CRISP DC HIE Tool Webinars



Webinars	Date/Time
Provider Directory	Wednesday, June 10th 12:00PM-1:00PM
Image Exchange	Tuesday, June 16th 12:00PM-1:00PM
Panel Processor	Thursday, June 18th 12:00PM-1:00PM
HIE Admin	Thursday, June 25th 12:00PM-1:00PM

Thank you!