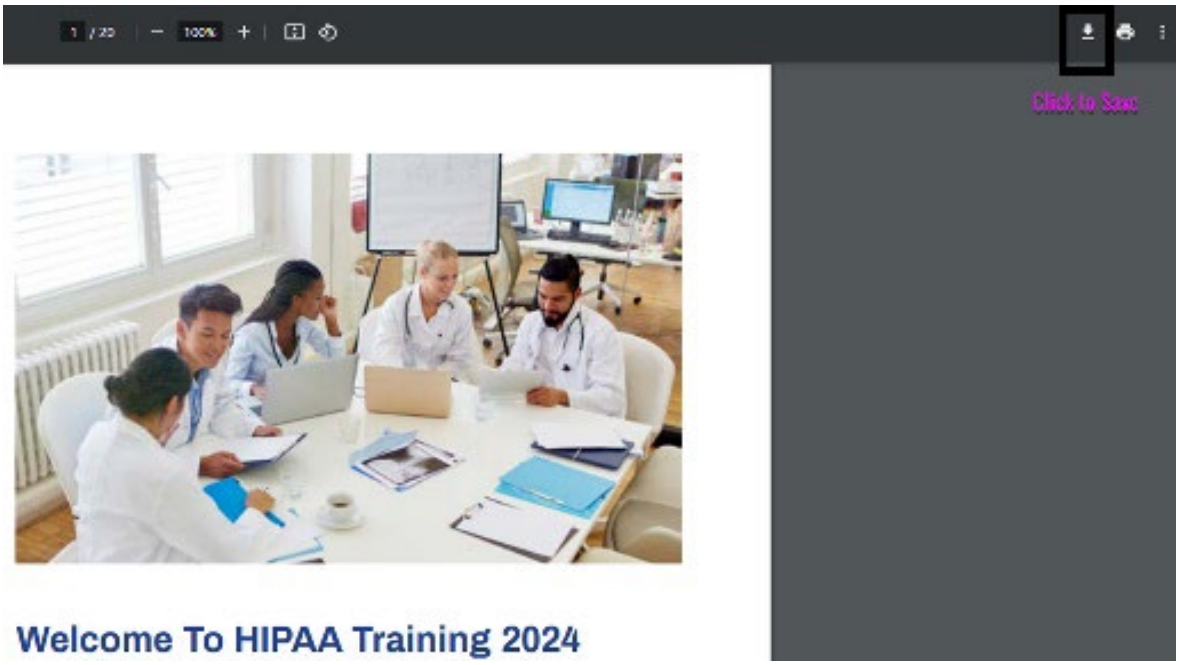
Staff Member Instructions

HIPAA Training 2024

1. Open the HIPAA Training 2024 pdf by right clicking on the file and choose: “Open with Google Chrome”.
2. Complete the training by reading the document and answering all questions.
3. Save your work by clicking on the down arrow, “save with changes” and save using your name and date of completion.
   Example File Name: michaelmccoy02262024



4. Once saved, email the completed pdf back to your HIPAA Compliance Officer. Write down any questions you may have for the HIPAA Compliance Officer to review later.

Welcome To HIPAA Training

This training manual is designed to be a fast paced review of the HIPAA Privacy Rule, Security Rule and Breach Notification Rule.

Healthcare Cybersecurity, The Value of Data

Healthcare data holds immense value for cybercriminals due to its rich and sensitive nature. The increasing prevalence of electronic health records (EHRs) has made healthcare systems vulnerable to ransomware attacks. The illicit sale of medical records and prescription information on the dark web can be used for insurance fraud, illegal prescription drug sales, or even extortion. Protecting healthcare data is crucial not only to safeguard individual privacy but also to prevent the potential financial and physical harm that it could cause.

Practice

HIPAA Compliance Officer

Social Engineering - CISA Guidance

In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network.

Medical Records can sell for hundreds of dollars each on the dark web.

Security Tips - Use these security tips at work and at home.

Think Before You Click.

Do not multi-task while checking email and review the return email address.

Use Complex/Strong Passwords.

Passwords are an important part of your Online security.

Characteristics of a Complex/Strong Password

- 12 to 16 characters. The longer the better.
- Upper and Lower Case Letters.
- At Least 2 Numbers.
- At least one symbol.

Security Tips - Cont.

Learn How To Spot Phishing Emails.

Be Aware of the Tactics Criminals Use to Trick You.

Never Use Free WiFi If You Have PHI on Your Phone or Connect to a Network with PHI.

Free WiFi can be hijacked by criminals and Expose Your Devices and Data.

Follow Your Policies and Procedures

They Are To Help Protect Your Information and Patient Information.

Know How To Detect and Report Suspicious Incidents -

Report Suspicious Activity Immediately.

Do Not Install Software, Instant Messaging or Other Apps Without Supervisor and IT Approval.

Be Wary of Unexpected Requests for Personal Information

Your IT Vendor will not ask you for your password and Microsoft never calls you.

Hover Over Attachments Before Opening or Downloading & Review.

By hovering over links you can see where the link will take you.

Do Not Open/Click/Respond Unless You Are 100% Sure.

If you have any suspicions or doubts, check with IT.

Show Your Knowledge

1. A "social engineer" may try to trick me into disclosing my password.

   True ☐ False ◯

2. It is safe to access patient information when accessing the internet on "Free" WiFi.

   True ☐ False ◯

HITECH Compliance Associates, Inc.

3905 Tampa Road, Suite 213
Oldsmar, Florida 34677
Direct Questions to michaelmccoy@hipaack.com
or call us at: 813-892-4411

About HITECH:

HIPAA consulting firm specializing in HIPAA Risk Assessments, HIPAA Training, Policies and Procedures, Breach Documentation and Comprehensive Support for HIPAA compliance.

The Facts About Phishing

Deceptive Emails Are A Threat In the Workplace and At Home

Every day 3.4 billion phishing emails get sent out. Cyber criminals use malicious email to scam medical practices and individuals. They play on your emotions and the fact that you are busy to trick you into responding to emails that:

1. **Contain Malicious Web Links** - asked to click on a link that takes you to an infected website.
2. **Malicious Attachments** - urged to open an attachment which contains malware, and
3. **Fraudulent Data-Entry Forms** - the email prompts you for sensitive information such as passwords.
4. **Promt to Call Customer Service** - They request your password to verify your identity.

Phishing can affect you at home as well.

Consequesces of Falling for a Phishing Email

Work	Personal Life
Loss of practice funds	Money stolen from your bank accounts
Exposed employment of staff	Credit card fraud
Criminals accessing patient information	False tax returns filed in your name
Being locked out of your computers	Loss of your personal photos, video and files
Loss of professional reputation	Fake social media posts made under your account

Phishing Email is an attack that attempts to steal your money, or your identity, by getting you to reveal personal information on websites that pretend to be legitimate.

Common Email Fraud Subject Lines

- Request
- Urgent
- Payment
- IRS
- Payroll Related

Common Phishing Scam Tactics

- Fake Invoices
- Password Reset
- Mail Delivery Failure
- UPS/FedEx/Postal Delivery Problem
- PDF and Word Attachments that are Malicious
- Order Conformation
- Employment Opportunity
- We Value Your Opinion - Just answer 2 questions for a $50 Amazon Gift Card

Ways to Spot A Phishing Email

- Mismatched Email Domains - Return Email Address
- Email or text message from bank to verify transaction or your account has been suspended.
- Generic Greetings
- Bad Grammer
- Urgent Call to Action or Threat
- First Time Sender
- Request Phone Call To Verify Purchase
- Phone Number to Call is Prominent

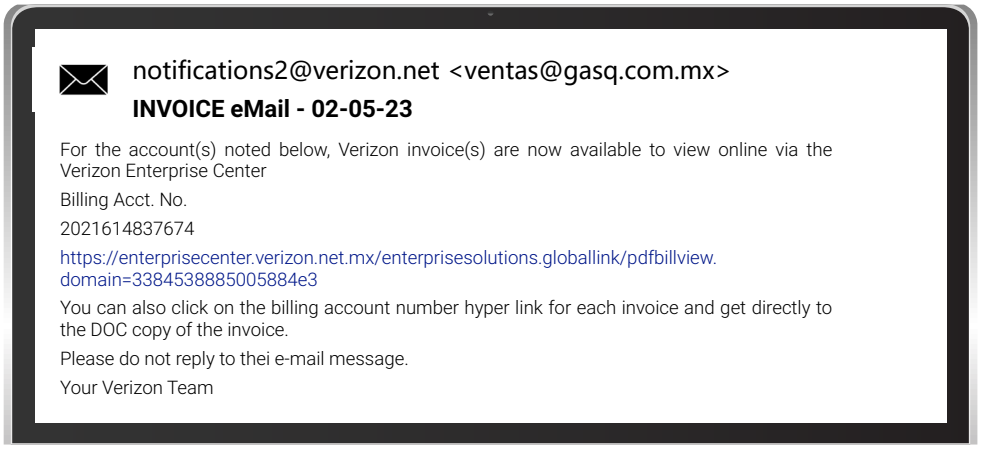
Show Your Knowledge

3 List 2 Common Email Fraud Subject Lines.

4 List 2 Common Phishing Scam Emails

Phishing Examples

1. Malicious Web Link



notifications2@verizon.net <ventas@gasq.com.mx>

INVOICE eMail - 02-05-23

For the account(s) noted below, Verizon invoice(s) are now available to view online via the Verizon Enterprise Center

Billing Acct. No.

2021614837674

https://enterprisecenter.verizon.net.mx/enterprisesolutions.globallink/pdfbillview.domain=3384538885005884e3

You can also click on the billing account number hyper link for each invoice and get directly to the DOC copy of the invoice.

Please do not reply to thei e-mail message.

Your Verizon Team

Think Before You Click.

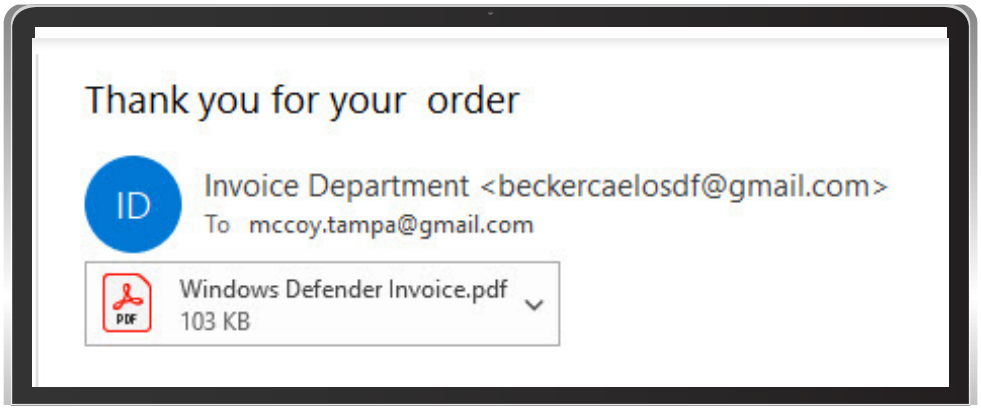
Does the return email match the sender's name?

Note the .mx at the end of the email address. That is a country code sending this email to Mexico.

Read the email. Does it sound right?

Hover over the "Release Messages Now". Where is the address sending you to?

2. Malicious Attachment



Thank you for your order

ID

Invoice Department <beckercaelosdf@gmail.com>

To mccoy.tampa@gmail.com

Windows Defender Invoice.pdf

103 KB

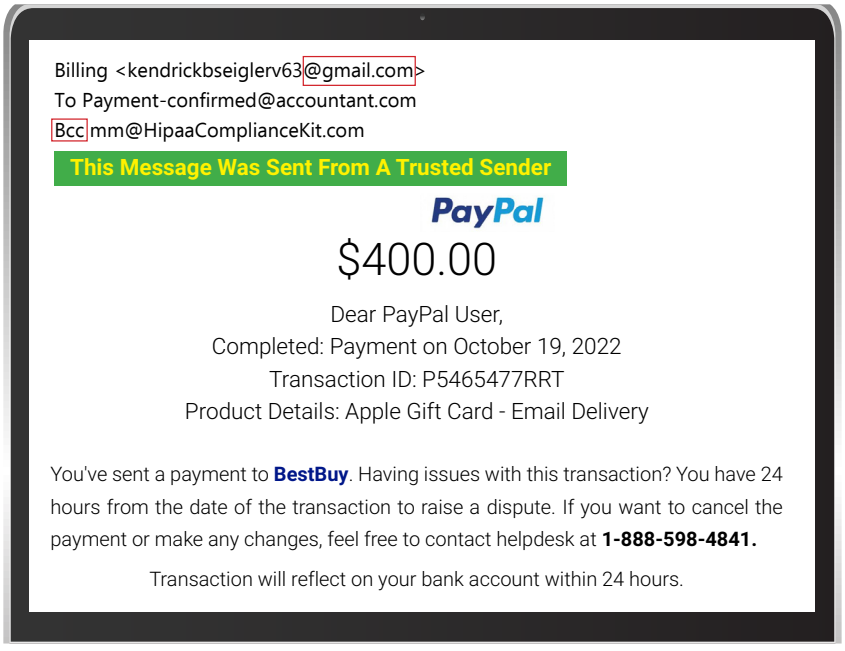
Think Before You Click.

This is a fake invoice. Do not be tricked into seeing what you are being billed for and open the PDF.

Common Attachments:

- PowerPoint
- Word
- Excel
- PDF

3. Prompt to Call



Billing <kendrickbseiglerv63@gmail.com>

To Payment-confirmed@accountant.com

Bcc mm@HipaaComplianceKit.com

This Message Was Sent From A Trusted Sender

PayPal

$400.00

Dear PayPal User,

Completed: Payment on October 19, 2022

Transaction ID: P5465477RRT

Product Details: Apple Gift Card - Email Delivery

You've sent a payment to **BestBuy**. Having issues with this transaction? You have 24 hours from the date of the transaction to raise a dispute. If you want to cancel the payment or make any changes, feel free to contact helpdesk at **1-888-598-4841.**

Transaction will reflect on your bank account within 24 hours.

Think Before You Click.

Does the return email match the sender's name?

Did the email come from a gmail or yahoo account?

Read the email. Does it sound right?

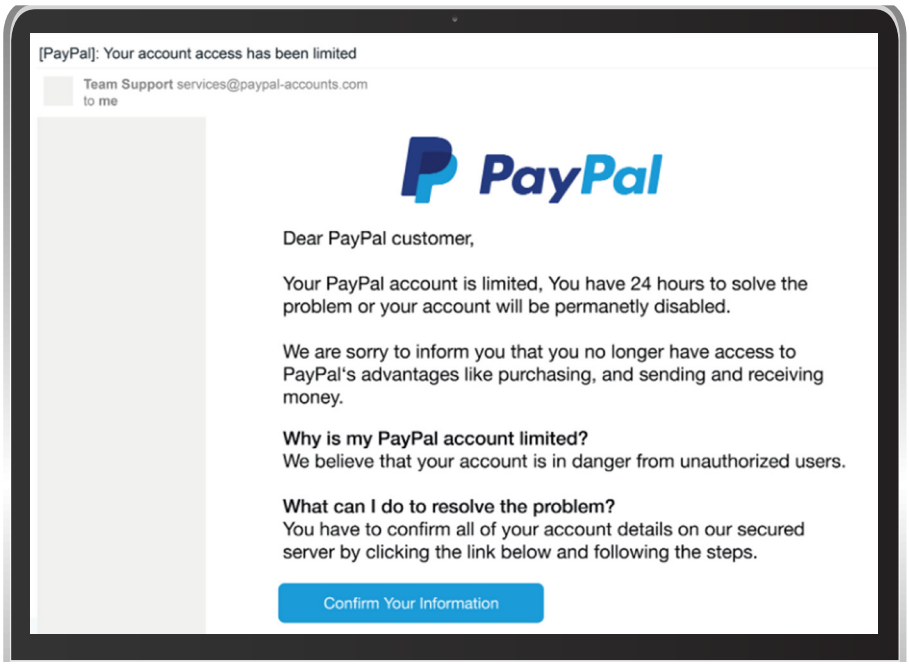
Don't be fooled because it contains a "real" logo.

Bcc - This email was sent to other receipents but only your email address shows.

Bold phone number encourages you to call to get this corrected.

Sense of Urgency, only 24 hours to correct.

General greeting, Dear PayPay User.



Think Before You Click.

Do Not Multi-Task, this is an easy email to see and click without reviewing.

Sense of Urgency, your not receiveing emails.

Hover over the "Confirm Your Information". Where is the address sending you to?

Confirming Your Information will give your credentials to cybercriminals.

Show Your Knowledge

5 When reviewing emails, I should always check the return email address.

True ☐ False ◯

6 Falling for a phishing email could allow criminials to access my bank account(s).

True ☐ False ◯

Password Security - Guidance FBICYBER and CISA

We all use passwords to secure our phones, computers, email, and online accounts. Unfortunately, many of us use—and reuse—simple passwords because they are easier to remember. However, malicious cyber actors commonly exploit simple, weak passwords to obtain users' login information. Passwords only work if they are complex/strong and confidential. Many practice's have been successfully breached because of non-secure and inadequate passwords. Once a system is compromised, it is open to exploitation by other unwanted sources.

Common Password Attacks

Dictionary Attacks

Dictionary attacks work because many computer users insist on using ordinary words as passwords. Dictionary attacks also includes all passwords from previous breaches.

Brute Force Attacks

Short passwords or character patterns, such as Summer1993 and a1b2C#, are commonly used and relatively easy for an adversary's computer to crack with modern tools.

You can implement the following best practices to prevent these types of attacks.

- **Do not save your passwords in browsers per CISA guidelines.**
- **Use different passwords on work and personal accounts.**
- **Use the longest password or passphrase permissible by each password system.**
- **Consider using a password manager program to keep track of your passwords. (See List)**
- **Do not use passwords that are based on personal information that can be easily accessed or guessed.**
- **Do not use words that can be found in any dictionary of any language.**

Use Multi-Factor Authentication (MFA).

Enabling MFA is easy and boosts security significantly as it requires an extra layer of identity verification before you can gain access to an account. Ask HIPAA compliance officer for more information.

Show Your Knowledge

7. Password Managers are a good tool to keep information private.

   True ☐ False ◯

8. List one best practice for password security.

What Makes a Password Complex

Start with 3 Unrelated Words

witty apple axe

w1tty@pPl71eAxe

❶ ❷ ❸ ❹

1) Substitute a Number for a Letter
2) Use a Symbol in Your Password
3) Add at Least 1 Capital Letter
4) Add at Least 2 Random Numbers

Use a **Minimum of 15 Characters**, add length for a stronger password.

Websites To Improve Security

https://haveibeenpwned.com/- Check your user ID (email address) and see if your password is compromised.

Password Managers: https://1password.com/; **https://bitwarden.com**/; **https://www.dashlane.com/**

Internet Use Policy

The INTERNET is a very dangerous place. You must be protected with premium anti-virus if you want any chance of staying safe and protecting your practice and yourself. (Find affordable anti-virus at **www.newegg.com**) Bitdefender, Web Root, Malwarebytes Pro are just a few examples of great anti-virus. Employees are expected to use the Internet responsibility and productively. Internet Access is limited to job-related activities only and any personal use is not permitted. **Do Not:**

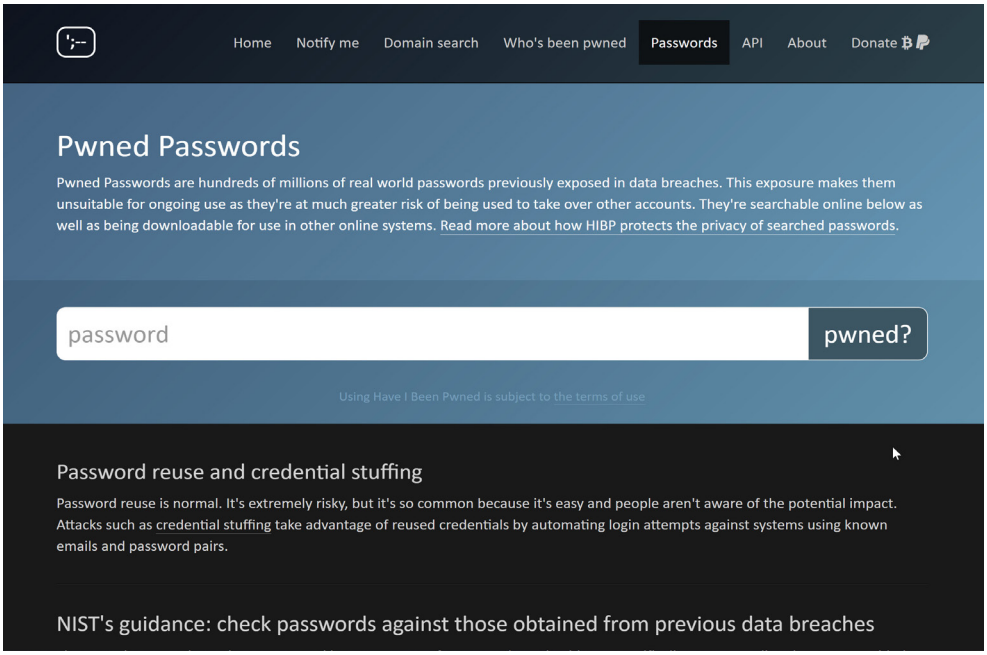
- Go to Social Media Web sites
- Go to News Web Sites
- Look Up Celebrities

and never

- Go Open Your Own Personal Email on a work computer.
- Use your own personal device that is not on the Practice WiFi Network.

Social Media Policy

HIPAA does not allow our practice to respond to social media posts. No matter how much information a patient posts or what they say, you cannot respond. The fines for responding to social media posts range from $30,000 to $50,000. Bring any concerns you may have directly to the HIPAA Compliance Officer.



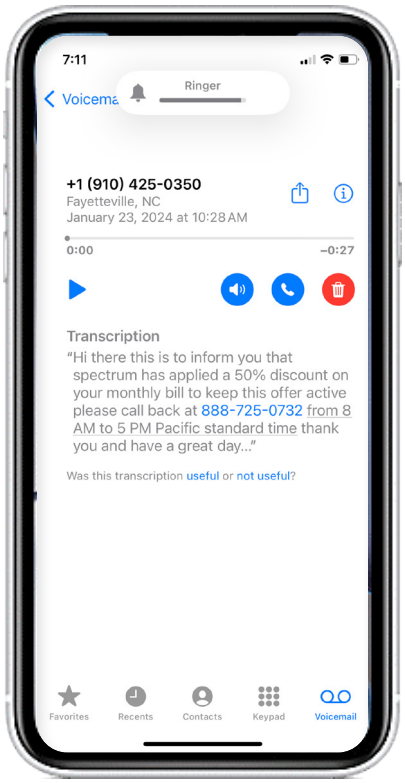
Cyber Safety is Patient Safety

Show Your Knowledge

9 It is OK to check my personal email account at work. True ◯ False ☐

10 Responding to social media posts about your practice is required. True ◯ False ☐

THE RISKS OF USING A MOBILE DEVICE



Mobile devices in general aren't as secure as computers.

In addition to loss and theft, there are many other ways a mobile device could be harmful to protected health information (PHI). Other risks include lack of authentication, mobile malware, unsecured Wi-Fi networks, outdated operating systems, and accidentally disclosing data.

No matter the type of technology a healthcare provider uses, they are obligated to protect PHI. If a smartphone or tablet is used to access, transmit, receive, or store information, it must have certain security precautions in place.

Make sure you get with your HIPAA Compliance Officer to reviw and sign a Mobile Device Policy.

For More Information on Securing Mobile Devices: **https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html**

What is a Smishing Attack? CISA Guidance

Smishing is a form of social engineering that exploits SMS, or text, messages. Text messages can contain links to such things as webpages, email addresses or phone numbers that when clicked may automatically open a browser window or email message or dial a number. This integration of email, voice, text message, and web browser functionality increases the likelihood that users will fall victim to engineered malicious activity.

Once a machine/mobile device has been compromised, the attacker can view the screen, access all files, capture access credentials, download passwords stored in the browser, take pictures using the machine's built-in webcam, record audio via the microphone, and access whatever data the user has access to. The attacker can even use the compromised machine as a pivot point to exploit other machines on the network from behind the firewall.

Show Your Knowledge

11 A Smishing attack could lead to a compromise of medical records.
True ◯ False ☐

12 If I use my personal device to send or receive patient information I need to sign a Mobile Device Policy with my practice. True ◯ False ☐

Never share your password or User ID, it is your digital identity.

General Tips on How to Avoid Being A Victim

Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, verify his or her identity directly with the company.

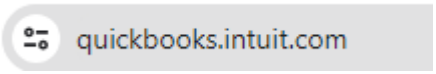
Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.

Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email or text messages.

Don't send sensitive information over the internet before checking a website's security or insuring email is encrypted.

Look for web address (URLs) that begin with "https"—an indication that sites are secure—rather than "http."

Click on this symbol and click to see if the site is secure.



If you are unsure whether an email request is legitimate, verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information.

Use multi-factor authentication (MFA). See HIPAA Compliance officer.

If You Believe You Are A Victim of A Phishing Attack

- Immediately Report To Your Supervisor and/or IT.
- Change Your Passwords (see how to create and use complex/strong passwords).
- Monitor your checking, credit cards and other accounts.
- Watch for signs of Identity Theft.
- Create an IRS PIN number. (**https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin**)
- Report the incident to police and FBI (**https://www.ic3.gov/Home/ComplaintChoice**)

Show Your Knowledge

13 Which website address is safer: https or http?

14 It is safe to give out my password if the request is in an email.

True ◯ False ☐

Minimum Necessary Standard - The Heart of HIPAA

The **Minimum Necessary Standard** is a key protection of the HIPAA Privacy Rule. It is based on accessing or disclosing protected health information only when it is medically necessary to satisfy a particular purpose or carry out a function. The minimum necessary standard requires covered entities and business associates evaluate their organization and enhance safeguards that limit unnecessary or inappropriate access to and disclosure of PHI. The Privacy Rule's requirements for minimum necessary are designed to be sufficiently flexible to accommodate the various circumstances of any business. The Minimum Necessary Standard requires all staff members utilize the same procedures to access their own and/or family and friends PHI in the same manner as patients would be required. When requesting charts from other offices only request the information needed for it's intended medical purpose.

Don't ask for the whole chart if you do not need the whole chart.

Just because you have access, does not give you the right to access.

Sensitive Protected Health Information (sPHI)

Take extra care with information that could cause financial, reputational or emotional damage to the patient.

Additional Protections for sPHI:

Even though a patient may have agreed to have a family member present when you are discussing the patient's general health, you should always check with the patient before discussing highly confidential information in the presence of family and/or friends.

While a patient may have given you permission to leave messages on an answering machine, you should never leave a message asking the patient to return a call concerning sPHI.

REMEMBER: Sensitive Protected Health Information requires an additional action by the patient before disclosing the information, even if the patient authorizes the entire file be sent to another office or third party.

Sensitive Protected Health Information (sPHI) includes:

- Psychotherapy Notes (which are not part of the official medical record)
- Information about a Mental Illness or Developmental Disability
- Information about HIV/AIDS Testing or Treatment
- Information about Communicable Diseases
- Information about Substance (i.e., alcohol or drug) Abuse
- Information about Genetic Testing
- Information about Child Abuse and Neglect
- Domestic Abuse/Violence
- Information about Sexual Assault
- Reproductive Health Information

Show Your Knowledge

15 Name the HIPAA standard that limits unnecessary or inappropriate access to and disclosure of PHI.

16 List 2 Examples of Sensitive Protected Health Information.

"HIPAA Should Not Get In The Way Of The Best Interests of the Patient." OCR

Privacy Rule Fast Facts for Covered Entities - HHS Guidance

The Privacy Rule does not require you to obtain a signed consent form before sharing information for treatment purposes. Health care providers can freely share information for treatment purposes without a signed patient authorization.

The Privacy Rule does not require you to eliminate all incidental disclosures. The Privacy Rule recognizes that it is not practicable to eliminate all risk of incidental disclosures.

The Privacy Rule does not cut off all communications between you and the families and friends of patients. As long as the patient does not object, The Privacy Rule permits you to:

- share needed information with family, friends, or anyone else a patient identifies as involved in his or her care;
- disclose information when needed to notify a family member or anyone responsible for the patient's care about the patient's location or general condition;
- share the appropriate information for these purposes even when the patient is incapacitated if doing so is in the best interest of the patient.

The Privacy Rule does not prevent child abuse reporting. You may continue to report child abuse or neglect to appropriate government authorities.

The Privacy Rule is not anti-electronic. You can communicate with patients, providers, and others by e-mail, telephone, or facsimile, with the implementation of appropriate safeguards to protect patient privacy.

Read the full document at: **https://www.hhs.gov/hipaa/for-individuals/family-members-friends/index.html**

Show Your Knowledge

17 HIPAA does not allow our office to report suspected child abuse.

True ☐ False ◯

18 As long as the patient does not object, I can share patient information with friends and family.

Ture ☐ False ◯

Sanctions Policy

The HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") require covered entities to ensure that workforce members comply with the HIPAA Rules. Regulated entities are responsible for protecting the privacy and security of protected health information (PHI) by training their workforce, adopting written policies and procedures, and sanctioning workforce members who violate those policies and procedures.Sanction policies are specifically required by both the Privacy Rule and the Security Rule.

Show Your Knowledge

19 My home network is too small to be the focus of a cyber criminal.

True ◯ False ☐

20 A violation of practice policies and procedures could end up with me receiving a:

HIPAA Breach Notification Requirements

Identifying a Breach.

If you think it's a breach, it is a breach. Really, HIPAA defines a **suspected breach as an actual breach** until your organization performs a ***Breach Security Risk Assessment*** and determines that no breach occurred.

HIPAA Omnibus Definition of a Breach

A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised.

As a workforce member it is your responsibility to ensure that any disclosure of patient information that is not allowed by the HIPAA.Omnibus regulations is documented and reported to your HIPAA Compliance Officer. Unless there is a patient emergency, reporting a breach is your top priority. Immediate response can help your organization mitigate any harm the breach could cause and may reduce the number of patient records disclosed.

Common Breaches That Must Be Reported

- Faxing PHI to the incorrect fax number/doctor's office.
- Giving an Encounter Summary or other patient records to the wrong patient.
- Mailing PHI to the incorrect address & it is returned with evidence it was opened.

Incidental Disclosure

Every risk of disclosure cannot be eliminated in your office.

HIPAA allows for *incidental disclosure* as long as your organization has **implemented reasonable safeguards and applied the minimum necessary standard**. Incidental disclosure occurs when a proper disclosure is being made and another patient or staff member not involved in the patient's care overhears or oversees PHI. The HIPAA Privacy Rule is not intended to impede these customary and essential communications and, thus, does not require that all risk of incidental use or disclosure be eliminated. Rather, the Rules permit certain incidental uses and disclosures of PHI to occur when the covered entity has in place reasonable safeguards with minimum necessary policies and procedures to protect an individual's privacy. Use additional safeguards when sensitive PHI is involved such as lowering your voice and talking behind closed doors.

Show Your Knowledge

21 I do not need to report a suspected breach, I only report known breaches. True ◯ False ☐

22 If a patient overhears another patient prescription information, that is an example of a _____ disclosure.

There is no privacy without Security

Privacy Rule - Patient's Rights

Requested Amendments to Protected Health Information

The Privacy Rule grants individuals the right to **request** amendments to their protected health information. Generally, a CE must honor the request unless it has determined that the information is accurate and complete. If the record is deemed to be correct your office can deny this request. You must send the patient a letter stating the reason for the denial.

Right to Request Confidential Communications

HIPAA states that your practice must accommodate reasonable requests for alternative communications such as mailing to a P.O. Box or only calling the patient on their cell phone. Note: Make sure this information is documented so that billing, appointment setters and others will not send information to the wrong address or call the wrong phone number.

Show Your Knowledge

23 A patient has a right to get their statements sent to their P.O. Box.

True ◯ False ☐

24 The Privacy Rule grants individuals the right to request changes to their PHI.

True ◯ False ☐

Patient's Rights to Access Their Medical Records

OCR Access Guidance

Patient's Have a Right To Access ALL PHI Maintained by Your Practice

Patients have access to their "designated record set" which includes Medical records and billing records about individuals maintained by or for a covered health care provider; enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or other records that are used, in whole or in part, by or for the covered entity to make decisions about individuals.

Patient's Right to Digital Copies of Theri Records Including A Patient's Right To Have A Right to Have Records Emailed To Themselves or Direct to Others

Email is generally considered readily producible by all covered entities. If the individual requested that the covered entity transmit the PHI in an unsecured manner (e.g., unencrypted), and, **after being warned of the security risks** to the PHI associated with the unsecure transmission, maintained her preference to have the PHI sent in that manner, the covered entity is not responsible for a disclosure of PHI while in transmission to the designated third party, including any breach notification obligations that would otherwise be required. Further, a covered entity is not liable for what happens to the PHI once the designated third party receives the information as directed.

Allowable Fees for Medical Records

The Privacy Rule permits a covered entity to impose a reasonable, **cost based fee** if the individual requests a copy of the PHI. The fee may include only the cost of:

(1) labor for copying the PHI;

(2) supplies for creating the paper copy or electronic media (USB drive);

(3) postage.

Time Limits to Grant Access/Copies

Access to the individual must be provided no later than 30 calendar days from receiving the individual's request. **The 30 calendar days is an outer limit and covered entities are encouraged to respond as soon as possible.** Indeed, a covered entity may have the capacity to provide individuals with almost instantaneous or very prompt electronic access to the PHI.

Verification is Required and Must be Documented

The Privacy Rule requires a covered entity to take reasonable steps to verify the identity of an individual making a request for access. Verification by be in written or oral form and must be documented.

You Cannot Require Patients to Use Your Portal.

It is their choice on how to request and receive recrods.

Show Your Knowledge

25 I am not allowed to email patient records even if the patient requests me to.

True ◯ False ☐

26 Patients cannot be required to use our portal to get their medical records.

True ◯ False ☐

Communicating with Family & Friends

HIPAA is a Valve, Not a Blockage

OCR GUIDANCE STATES:

Even though HIPAA requires health care providers to protect patient privacy, providers are permitted, in most circumstances, to communicate with the patient's family, friends, or others involved in their care or payment for care. This guide is intended to clarify these HIPAA requirements so that health care providers do not unnecessarily withhold a patient's health information from these persons. This guide includes common questions and a table that summarizes the relevant requirements.

COMMON QUESTIONS ABOUT HIPAA

1. If the patient is present and has the capacity to make health care decisions, when does HIPAA allow a health care provider to discuss the patient's health information with the patient's family, friends, or others involved in the patient's care or payment for care?

If the patient is present and has the capacity to make health care decisions, a health care provider may discuss the patient's health information with a family member, friend, or other person if the patient agrees or, when given the opportunity, does not object. A health care provider also may share information with these persons if, using professional judgment, he or she decides that the patient does not object. In either case, the health care provider may share or discuss only the information that the person involved needs to know about the patient's care or payment for care.

Example:

- Your doctor may talk to your sister who is driving you home from the hospital about your keeping your foot raised during the ride home.

BUT:

- A nurse may not discuss a patient's condition with the patient's brother after the patient has stated she does not want her family to know about her condition.

Read the full document at: **https://www.hhs.gov/hipaa/for-individuals/family-members-friends/index.html**

More HIPAA and Security Training:

Go to our YourTube Channel: **HIPAA TV**

Access Our HIPAA Training Video at:
https://youtu.be/FZrpkceNCVk?si=n2phwVlqczURb_Xx

Releasing Medical Records:
https://youtu.be/0BMUkj2leHc

Download HIPAA Essentials at
www.HipaaComplianceKit.com

Web Site To Review

www.newegg.com
www.haveibeenpned.com

Show Your Knowledge

27 Unless the patient has put a family member or friend on their Confidentiality List, I cannot talk to them about the patient's health care.

True ◯ False ☐

Medicare Fraud and Abuse

Fraud is an intentional act of deception, misrepresentation, or concealment in order to gain something of value.

Waste is over- utilization of services (not caused by criminally negligent actions) and the misuse of resources.

Abuse is excessive or improper use of services or actions that are inconsistent with acceptable business or medical practice. While not fraudulent, abuse may directly or indirectly ca use financial loss.

Our practice maintains Policies and Procedures that support the Compliance Program objectives. Billing practices are dedicated to keeping abreast of documentation and coding changes and updates over time so that claims are accurate.

Additionally, the Compliance Program is committed to abiding by relevant laws and ensuring that our employees and associates are not included on the OIG List of Excluded Individuals/ Entities.

The False Claims Act, or FCA.

Prohibits presenting or causing to be presented to the federal government a false or fraudulent claim for payment or approval. The FCA was amended in 2009 to expand the scope. The Anti- Kickback Statue. This statue makes it a criminal offense to knowingly and willfully offer, pay, solicit, or receive any remuneration to induce or reward referral of items or services reimbursable by a Federal health care program.

The Beneficiary Inducement Statute prohibits certain inducements to Medicare beneficiaries. For example, **coinsurance and deductible amounts will not be waived unless it is determined in good faith that the individual is in financial need and reasonable collection efforts have been made.**

Self- Referral Prohibition Statue (Stark Law). This law prohibits physicians from referring Medicare patients to an entity with which the physician or physician' s immediate family member has a financial relationship, unless an exception applies.

Reporting

Employees are encouraged to report any concerns of compliance issues to the Compliance Officer. Reports may also be made anonymously to any manager. An employee may make a report via verbal discussion, email, or voicemail. At no time will there be any form of retribution to any employee who reports possible compliance violations in good faith.

Disciplinary Action

Disciplinary action will be imposed upon any employee for failing to comply with and adhere to standards, policies, and applicable statues or government regulations. Intentional or reckless noncompliance may result in the employee' s termination. All levels of employees will be subject to the same types of disciplinary action for the commission of similar offenses.

Show Your Knowledge

28 An honest mistake in billing is considered Medicare Fraud.

True ◯ False ☐

29 If I suspect Medicare Fraud, I should not report it to my supervisior because it could cause problems for the practice.

True ◯ False ☐