

HIPAA in 30

Innovative, fast paced training for HIPAA

**HIPAA Privacy Rule
Healthcare Cybersecurity
Breach Notification Requirements
Information Blocking**



View the Companion Video at:
<https://youtu.be/FZrpkceNCVk>
or scan the QR Code



HIPAAessentials
TRAINING

HITECH Compliance Associates, Inc.

HIPAA

The HIPAA Privacy Rule

HIPAA establishes a foundation of Federal protections for Protected Health Information (PHI). The Omnibus Rule added new patient right's, changes in breach reporting and other requirements your practice must understand and implement.

The HIPAA Security Rule

The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity and/or business associate.

The HIPAA Breach Notification Rule

The Breach Notification Rule has reporting requirements to patients and the Office for Civil Rights to ensure notification if their PHI is seen or disclosed to those outside of need to know.

OCR Patient Access Initiative

Right To Get All Medical Records In Their Designated Record Set

Patients have a right to all the records your office has pertaining to their care including records you may have from other offices. Due to the new Information Blocking laws all digital records need to be available immediately through the patient portal.

Right to Get Medical Records in Digital Format Requested/Available

Patients have a right to get their medical records on digital format that includes digital media and email. Never accept a patient's thumb drive or send ePHI via email without warning the patient of the risks.

Right To Be Verified Over the Phone

Patients do not have to come into your office to request records. Your office must have a method to verify a patient. It is important to document that you verified the patient's identity with your established verification questions.

Right To Records For A Flat Fee, Up To \$6.50 or Worksheet of Costs

State pricing does not apply unless it is less expensive than the above costs.

Right to Access and Inspect Copies of their Designated Record Set

Patients have a right to sit at a workstation in your office and view their records in the EMR. You cannot charge for this service.

Information Blocking

is a law that went into effect on April 5, 2021. Information Blocking requires immediate release of EHI upon request by a patient, their personal representative or a continuity of care provider. HIPAA permitted you to share the records, Information Blocking requires the sharing of records. For more guidance on Information Blocking please review our "Getting Started with Information Blocking" publication and go to our You Tube Channel: HIPAA TV and review the videos on Information Blocking and HIPAA training.



HIPAA in 30

1 HIPAA is Federal Law

composed of the:

HIPAA Privacy Rule

HIPAA Security Rule

Breach Notification Rule

These rules and regulations carry significant fines and penalties for practices & individual staff members.

2 HIPAA Protects PHI

Protected Health Information.

PHI is any oral, written or electronic individually-identifiable health information collected or stored by a HIPAA covered entity.

PHI consists of at least one identifier matched with TPO. (Treatment, Payment or Health

3 Minimum Necessary

The Minimum Necessary Standard, a key protection of the HIPAA Privacy Rule. It is based on sound, current practice that protected health information should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function.

4 Permitted Disclosures

A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization for purposes of Continuity of Care.

5 Right of Access

Patients have a right to access their entire designated record set, pay lower fees for records, get records in digital format, be verified over the phone for medical records requests and to access directly upon request.

6 Medical Records

With limited exceptions, the HIPAA Privacy Rule gives individuals the right to access, upon request, the medical & health information (protected health information) about them in one or more designated record sets maintained by or for the individuals' health care providers.

7 Medical Records Pricing

Patients can be charged a flat fee, up to \$6.50 or the Practice needs to use a worksheet showing how the price was calculated using the HIPAA allowable charges. Should a patient claim financial hardship, OCR recommends not charging the patient.

8 Digital Format

The Privacy Rule requires a covered entity to provide the individual with access to the PHI in the form and format requested, if readily producible in that form and format or as otherwise agreed to by the covered entity and individual.

HIPAA in 30

9 Emailing Required

Email is a digital format that can be requested by patients. Mail and e-mail are generally considered readily producible by all covered entities. It is expected that all covered entities have the capability to transmit PHI by mail or e-mail.

10 Verification

The Privacy Rule requires a covered entity to take reasonable steps to verify the identity of an individual making a request for access. Verification may be done orally. You need to document the request.

11 Direct Access

Patients have a right to see their medical records directly as you see them in the EHR. They can take photos of the screen. No charge can be applied for this access and you must accommodate within 30 days.

12 Denial of Access

Patients do not have a right to access their psychotherapy notes. Other denial can be applied for harm and other exemptions. Denials are divided into denial without review and denial with review.

13 Request to Amend

Individuals have the right to have covered entities amend their protected health information in a designated record set when that information is inaccurate or incomplete. If you agree, make the amendment, if you disagree, send a letter why you disagree.

14 Confidential Contact

Health care providers must permit individuals to request an alternative means or location for receiving communications of protected health information by means other than those that the covered entity typically employs.

15 Restrictions of PHI

A covered entity must agree to a request to restrict disclosure of PHI about the individual to a health plan if the individual has paid the covered entity in full.⁹ This may require that the patient receive a Good Faith Estimate for services.

16 Disclosures to Family

friends and caregivers. HIPAA allows health care professionals to disclose some health information without a patient's permission under certain circumstances.

Ask Permission

Give Opportunity to Object.

HIPAA in 30

17 Acting of Disclosures

Individuals have a right to an accounting of the disclosures of their PHI by a covered entity or the covered entity's business associates. All disclosures outside of TPO must be disclosed from the past 6 years. No charge is allowed.

18 Notice Privacy Practices

CE's must provide a Notice of its Privacy Practices. The notice must describe the ways the CE may use & disclose PHI. The notice must state the CE's duties to protect privacy, provide a notice of privacy practices, & abide by its terms.

19 HIPAA Security Rule

The Security Rule sets the standards of security controls all CEs and BAs must follow. The rule is flexible to allow different size entities to enact security that is reasonable and appropriate. It all starts with your Risk Analysis and Risk Management Plan.

20 Healthcare Cybersecurity

Awareness is the key to protecting your valuable data. All staff members need to be trained on common cybersecurity tactics such as phishing email and other social engineering techniques.

21 Phishing Email

Cybercriminals target your practice with email with malicious links and/or attachments. Always check the return email address to make sure it matches the sender's address. Do not multi task when reviewing email. Pay attention to what you click.

22 Social Engineering

Taking advantage of human behavior is the social engineer's tool. Trust but verify. When talking to anyone over the phone, know who you are talking to. Be limited with the information you give out and never give out your password over the phone.

23 Complex Passwords

Weak, non-complex passwords allow cybercriminals to guess your password with super fast computers. Make sure your password is 10 characters in length, uses upper and lower case letters, at least two numbers and a symbol.

24 Password Protections

Change your passwords every 90 days. Make sure you are using complex passwords to 1) log into your computer, 2) to log into software containing PHI and 3) do not forget email. Cybercriminals go after email to learn what attacks will work against your practice.

HIPAA in 30

25 Limit Internet Usage

The Internet is infected with malicious web sites. Land on one of these sites and your practice is compromised within a 1/2 second. Use the internet for work purposes only. Never access your personal email from a work computer, it's too dangerous.

26 Sending Email

Email must be encrypted if it contains any PHI. The only exception is when it is sent directly to the patient after the patient has been warned of the danger and the warning is documented in the email. No patient signature required.

27 HIPAA Breach

Any impermissible acquisition, access, use or disclosure of unsecured PHI is presumed to be a breach. Sending PHI to the incorrect physician's office or giving a patient another patient's discharge summary. Both must be documented with a Breach Risk Assessment.

28 Breach Risk Assessment

4 Questions Required by Federal Law. 1. What were the identifiers and TPO involved? 2) Who was the unauthorized disclosure made to? 3) Was the PHI actually viewed or acquired? 4) To what extent has the risk been mitigated?

29 Incidental Use

HIPAA does not require every risk of an incidental use or disclosure of PHI be eliminated. A use or disclosure that occurs as a result of, or as "incident to," a permitted use or disclosure is permitted. Reasonable safeguards & Minimum Necessary required.

30 Privacy vs. Care

HIPAA is a balance, providing good health care while maintaining the patient's privacy is your responsibility. Use your professional judgment, common sense and error towards providing the best patient care. Always document HIPAA concerns for your HCO.

Examples of Information Blocking

Except as required by law or covered by an exception, is likely to interfere with access, exchange, or use of electronic health information (EHI).

Requiring a signed Authorization to share records for Continuity of Care.

Creating Hurdles to Access or Exchange EHI.

Misunderstanding the law.

Applying (claiming) HIPAA restricts when no legal claim exists.

Slowing or Delaying

Taking more than a day or not having records immediately that had been "requested".

Communicating with Family & Friends

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.



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.

Here are some examples:

- An emergency room doctor may discuss your treatment in front of your friend when you ask that your friend come into the treatment room.
- A doctor's office may discuss a patient's bill with the patient's adult daughter who is with the patient at the patient's medical appointment and has questions about the charges..
- 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.
- Your doctor may discuss the drugs you need to take with your health aide who has come with you to your appointment.
- A nurse may discuss a patient's health status with the patient's brother if she informs the patient she is going to do so and the patient does not object.

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.
- A nurse may not tell a patient's friend about a past medical problem that is unrelated to the patient's current condition.
- A health care provider is not required by HIPAA to share a patient's information when the patient is not present or is incapacitated, and can choose to wait until the patient has an opportunity to agree to the disclosure.

HIPAA Exception: In order to prevent or lessen a serious and imminent threat to the health or safety of a person or the public to the person that can help mitigate the risk.

www.hhs.gov/hipaa/for-individuals/family-members-friends/index.html

The Importance of Complex Passwords in Medical Practices

Complex Passwords show our commitment to patient confidentiality and trust. Using easy-to-guess or common passwords is akin to leaving our patient files out in the open waiting room.


Managing multiple, complex passwords can seem daunting. However, considering the stakes it is essential to ensure that all of our passwords meet minimum complexity requirements. Our patients trust us with their most intimate health details, and we owe it to them, and to the reputation of our practice, to keep that trust intact.

One of the most common ways that hackers break into computers is by guessing passwords. Simple and commonly used passwords enable intruders to easily gain access and control of a computing device.

Conversely, a password that is difficult to guess makes it prohibitively difficult for common hackers to break into a machine and will force them to look for another target. The more difficult the password, the lower the likelihood that one's computer will fall victim to an unwanted intrusion.

USING CHATGPT HARDWARE TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	Instantly	Instantly	Instantly
8	Instantly	Instantly	Instantly	Instantly	1 secs
9	Instantly	Instantly	4 secs	21 secs	1 mins
10	Instantly	Instantly	4 mins	22 mins	1 hours
11	Instantly	6 secs	3 hours	22 hours	4 days
12	Instantly	2 mins	7 days	2 months	8 months
13	Instantly	1 hours	12 months	10 years	47 years
14	Instantly	1 days	52 years	608 years	3k years
15	2 secs	4 weeks	2k years	37k years	232k years
16	15 secs	2 years	140k years	2m years	16m years
17	3 mins	56 years	7m years	144m years	1bn years
18	26 mins	1k years	378m years	8bn years	79bn years

 [Learn how we made this table at hivesystems.io/password](https://hivesystems.io/password)

HIPAA Quick Reference Guide



Reasonable Safeguards to Protect Protected Health Information

- ...**Lower your voice when discussing patient information.**
- ...Do not discuss patient information in public areas including hall ways.
- ...Do not view your own medical record or those of family and friends without proper authorization from your supervisor or HIPAA Compliance Officer.
- ...Dispose of protected health information in designated shredding bins.
- ...Do not install software (screen savers, etc...) without written approval.
- ...Never go on Facebook or other social networks at the office and do not disclose patient information over the internet.
- ...Never attach a thumb drive or cell phone to your workstation's USB port without authorization from the HIPAA Compliance Officer.
- ...Never give out your password over the phone.
- ...Do not store passwords on your workstation or mobile device.
- ...If something makes you suspicious, report it immediately.
- ...Never access your personal email from the office network/computer.

Complex Passwords - Required

Passwords Need to be a Minimum of 12 characters, Upper and lower case, 2 numbers and a symbol.

Useful tips to for creating strong passwords and keeping your information secure.

Use a unique password for each of your important accounts (i.e. email and online banking).

Do not use personal information such as your name, age, date of birth, child's name, pet's name, or favorite color/song when constructing your password.

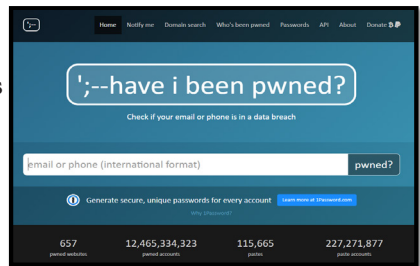
Avoid entering passwords when connected to unsecured WiFi connections (like at an airport or coffee shop) – hackers can intercept your passwords and data over unsecured connections.

Never tell your password to anyone, especially over the phone.

Change your passwords regularly and avoid using same password over and over again.

Never write down your passwords and hide underneath your workstation or telephone.

Do not save your passwords in your Internet browser.



How to Make a Password Complex

Start with 3 Unrelated Words: witty apple axe

w1tty@pPl71eAxe

① ② ③ ④

1) Substitute a Number for a Letter
3) Add at Least 1 Capital Letter

2) Use a Symbol in Your Password
4) Add at Least 2 Random Numbers

HIPAA Security Rule

Phishing Emails:

Deceptive Emails Are A Threat at Work and Home

BEWARE the Email w/ Attachments, Hyperlinks or Requesting Data.

Cyber criminals use deceptive emails to “fish for” information or secretly install dangerous software (malware) that compromises your computer and allows access to the files on it.

Phishing emails typically pressure you to act quickly, without thinking. They play on strong emotions such as curiosity, fear, and greed. These psychological manipulation tactics are known as “social engineering.”

Phishing Emails Steal Information Using the Following Methods:

Malicious web links – You’re asked to click on a link that takes you to an imposter website or to a site infected with malware.

Malicious attachments – You’re urged to open an unexpected attachment that contains malware.

Fraudulent data-entry forms – You’re prompted to fill in sensitive information like user IDs, passwords, credit card data, and phone numbers.

Email about a purchase - you did not make and call to correct.

Awareness & Learning How to Identify Common Attacks

Disguised phishing messages:

- Requests from the IRS or other tax bodies
- Software update notifications from trusted providers
- Alerts from known banks, retailers, social media outlets, etc.
- Notifications from internal departments like IT, HR, etc.

Thoroughly read emails. Watch for:

- ☒ Misspellings and poor grammar
- ☒ Messages that don’t seem quite right. (**Too Good to be True???**)
- ☒ Unsolicited emails

Web Sites to Review

Dark Web Search of Credentials
<https://HaveIBeenPwned.com/>

Password Manager -
<https://bitwarden.com/>
www.dashlane.com/

Check your password -
<https://www.passwordmonster.com/>

Home Network Security:
Firewalla.com

Send Secure Email:
sendinc.com

Create Temporary Email:
<https://10minutemail.com/>

Amazing New Technology
<https://openai.com/product/gpt-4>



Sample Phishing Emails

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.



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

Should you click on this link?

<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 the e-mail message.

Your Verizon Team

Reply Reply All Forward



Jennifer <JenniferXXXX@XXXXHealth.com>
Request for Wire Details

Dear Michael,

Good Day,

Kindly request you to share the wire transfer details to process your future payments at the earliest.

Thanks,

Jennifer
Senior- Business Development

Medicare Fraud & Abuse Examples

- Billing for services, supplies, or equipment that were not provided
- Billing for excessive medical supplies
- Obtaining or giving a Medicare number for “free” services
- Improper coding to obtain a higher payment
- Unneeded or excessive x-rays and lab tests
- Claims for services that are not medically necessary
- Using another person’s Medicare number, or letting someone else use your number

Notes: _____

Breach Notification Requirements

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.

Identifying a Breach.

If you think it’s a breach, it is a breach. If anyone sees patient information that does not need to see the patient information, it is a breach.

Common Breaches That Must Be Reported

- Faxing PHI to the incorrect fax number or 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.

Breach Risk Assessment - You Must Document:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the protected health information or to whom the disclosure was made;
3. Whether the protected health information was actually acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated.

