








Compliance

2025 HIPAA 101 | Privacy & Security

Training

HIPAA 101

-  HIPAA 101 | Privacy
-  The Privacy Rule
-  Compliance
-  Breaches
-  Enforcement
-  The HIPAA Privacy Rule Dos and Don'ts
-  HIPAA 101: Privacy | Summary

HIPAA 101- SECURITY



HIPAA 101 | Security



Security Rule



ePHI Access Monitoring



Safeguarding Against Cybersecurity Threats



Reporting Cybersecurity Incidents

HIPAA 101 | Privacy



The Health Insurance Portability and Accountability Act, or HIPAA, is a federal law that sets a minimum standard about how patient information must be protected and when it may be used or disclosed. Keep in mind that state laws, organization policies, and our payer contracts may include more restrictions than HIPAA. After this lesson, you should understand what the privacy rule is, who it applies to, and what protected health information is. You will learn how to comply with the rules and use and disclose patient information. You should also understand the requirements related to the minimum necessary standard and understand the patient's rights under HIPAA. You will learn what a breach of protected health information is, as well as what to do if you suspect a breach has occurred. You will also learn about how the privacy rule is enforced by the government, and you will learn your role in protecting PHI from within the organization. Let's get started.

Learning Objectives:

By the end of this section, you will be able to:

- Identify the steps you need to take to safeguard patient information.
- Report potential privacy incidents.

The Privacy Rule

PRIVACY RULE

The Privacy Rule **provides** appropriate **safeguards** to protect the privacy of **Protected Health Information (PHI)**. The rule also sets **limits** and conditions on the **uses** and **disclosures** that may be made of such **information** without patient authorization. The rule **gives patients** certain **rights** over their health information, including the right **to examine** and **obtain a copy** of their health records, and the right to **request amendments**.

Who does HIPAA apply to?



HIPAA Applies to Covered Entities

Health Care Providers*

Doctors, Hospitals, Medical Groups, Pharmacies, Labs, etc.

Health Insurance Plans

Private and Public Payers

*Only if they transmit information electronically

HIPAA Applies to Business Associates

- A business associate is a person or entity that performs certain functions or activities on behalf of a HIPAA Covered Entity and uses, accesses, or discloses protected health information as a part of that function or service.
- A business associate must have a signed Business Associate Agreement with the Covered Entity that they are performing services for.
- A subcontractor of a Business Associate that creates, receives, maintains, or transmits PHI is also a business associate.

[HHS defines Business Associates](#)



Covered Entity or Business Associate?

Review each card below to see how HIPAA identifies these areas.

Privia Medical Group

Privia Medical Group is a
Covered Entity.

Privia Care Center

Privia Care Centers are
Business Associates of
Privia Medical Group. In
limited situations, Care
Centers may also be
Covered Entities
themselves.

Privia Management
Company

Privia Management
Company is a **Business
Associate.**

Together We Form an Affiliated Covered Entity (ACE) or Organized Healthcare Arrangement (OHCA)



We Share a Notice of Privacy Practice

"For the purposes of complying with federal privacy and security requirements, [Privia has] designated themselves as an ACE and/or OHCA."

Together we are **ALL** jointly and individually responsible for the privacy and security of our patients' Protected Health Information.

What is PHI?

Let's go over the definition of protected health information, or PHI.

Protected health information is a combination of two parts that are required for the information at hand to be considered PHI.

The first part that is required for information to be considered protected health information is health information.

This is any information that relates to the past, present, or future physical or mental health or condition of that individual.

The second part that is required is an identifier. An identifier is any information that identifies an individual or may be used to identify an individual. Examples of identifiers include, but are not limited to, name, date of birth, contact or address information, phone number or email address, social security number, photographs, as well as any number that is associated with a particular patient, such as medical record number or insurance ID number.

It's important to note that identifiers can be very general when dealing with small populations. HIPAA recognizes zip codes in rural areas, as well as age or year of birth for patients over the age of 89, as identifiers.

Remember to always be careful when handling PHI.

Where is PHI Located?

Where can PHI be found?

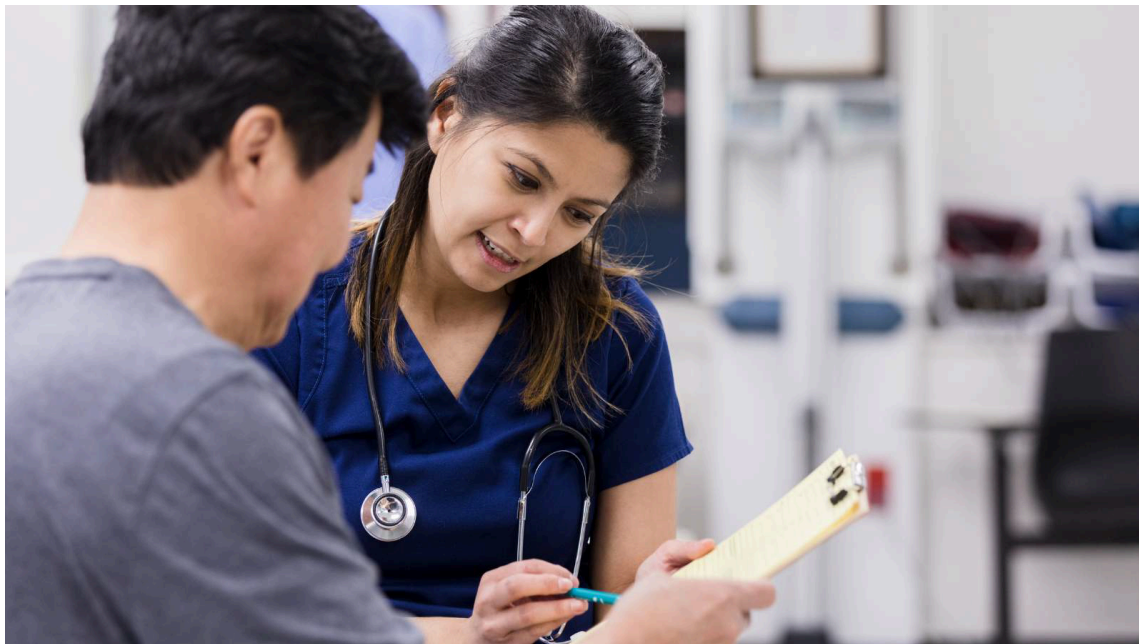
PHI can be found in paper records, within conversations, in electronic data, and anywhere patient health information and identifiers can be found.

PHI that is stored or transmitted electronically is considered ePHI, and has additional protections associated with it under the HIPAA Security Rule.

This includes information housed in the electronic health record, and information found on spreadsheets, e-mails, texts, or any other electronic or digital form.

PHI in any form should always be protected.

Compliance



Patient Authorization & Sharing PHI

As a general rule, HIPAA requires that we have patient authorization before using or sharing protected health information. An authorization is prior written permission from a patient to use or share that patient's PHI, unless we are doing so for what is known as a permitted purpose.

HIPAA allows the use or disclosure of protected health information (PHI) for three main permitted purposes without requiring prior written authorization from the patient:

1. **Treatment:** This includes coordinating care, consulting with other healthcare providers, referring patients, and other activities directly related to the patient's healthcare.
2. **Payment:** This covers activities such as billing, claims processing, eligibility verification, utilization review, and other actions necessary for receiving payment for healthcare services.
3. **Healthcare Operations:** This broad category encompasses a variety of activities that support the delivery of healthcare, including quality improvement, training programs, business planning, fundraising, and certain marketing activities.



Important Note: While these are the three main permitted purposes, HIPAA also allows for the use and disclosure of PHI without authorization in other specific situations, such as public health reporting, research, and disclosures required by law.

Key Rule | Minimum Necessary Standard

This standard applies whenever PHI is used or shared for non-treatment purposes. The standard requires us to take reasonable efforts to limit the amount of information that we use, request, or disclose to the minimum amount necessary to accomplish the intended purpose of the use, request, or disclosure.

Please note that the minimum necessary standard does not apply to those uses and disclosures made directly to the patient or their legal representative, as well as uses or disclosures made for treatment purposes, pursuant to a HIPAA authorization, or those required by law.

Under HIPAA, patients have the right to...

- **Access, copy** and **inspect** their health information.
- **Request** an amendment to their healthcare information.

- **Obtain** an accounting of certain disclosures of their health information (how their information was shared).
- **Request restrictions** on disclosures for treatment, payment of other healthcare operations.
- **Request** alternative means of **receiving communications** from covered entities.
- **Complain** about alleged violations of the regulations and the covered entity's own information policies.

Mandatory Requirements about the Notice of Privacy Practices (NPP)

Patients must be provided Privia's Notice of Privacy Practices (NPP)

All patients must be offered what is known as the Notice of Privacy Practices, or NPP, at their first visit or encounter, which outlines the rights provided to them under HIPAA, as well as important contact information for the patients, if they have questions or concerns about the privacy of their health information.

Posting of the Notice of Privacy Practices (NPP)

All Care Centers must prominently post the Notice of Privacy Practices (NPP) on their website. [Privia's NPP](#) is also available on the Privia website, and on the Privia app.

Breaches

What is a breach?

According to the HIPAA privacy rule, a breach is defined as the acquisition, access, use, or disclosure of protected health information, in a manner not permitted under the Privacy Rule, which compromises the security or privacy of the protected health information.

An impermissible use or disclosure of PHI is presumed to be a breach unless there is a low probability that the PHI has been compromised, and this is based on a detailed risk assessment. Only the Privia Privacy Officer can make the determination of whether or not an impermissible disclosure constitutes a breach of PHI.

Detect

Suspected Breach

- All Care Centers are required to report any incident or suspected breach to Privia's Privacy Officer, as soon as possible. All reports should be made no later than 3 business days after being made aware of the incident.
- Faster reporting typically leads to better investigation outcomes and mitigation.
- Mitigation strategies can be implemented to minimize harm to the patient and can reduce the financial risk for Privia Care Centers and Privia Medical Group.



Data breach

breach is the intentional
environment. Other

Respond

How to Report

To report an incident go to compliance.priviahealth.com from any web browser, including a mobile device. The more details you include about the incident, the faster we will be able to respond, potentially mitigate harm, and provide the appropriate notifications as required by law. If you have any questions you can email the compliance team at compliance@priviahealth.com.



Compliance, Privacy, and Security Incident & Suspected Breach Reporting

Recover

What we do next...

Following a breach of unsecured PHI, covered entities must notify the affected individual or individuals without unreasonable delay, and not later than 60 days after the discovery of a breach.

Health and Human Services (HHS) and the media must be immediately notified of any breach involving more than 500 individuals. Covered entities must file an annual report with HHS of all breaches involving fewer than 500 people.



	What is it?	How to Report	What to Include
Privacy Concerns	Any incident that involves any potential loss or inappropriate access of PHI.	Visit compliance.priviahealth.com Email compliance@priviahealth.com or privacy@priviahealth.com	<ul style="list-style-type: none"> • Date/Time of Incident • Details of the event including all systems involved • Best contact for investigation team to reach out to



A member of the Incident Response team will contact you to follow up on your report.

Enforcement

How is HIPAA Enforced?

The Department of Health and Human Services investigates all HIPAA complaints and breaches. The HHS Office of Civil Rights, or OCR, is the HIPAA Enforcement Agency. Any complaint or breach of PHI may subject Privia, and/or our care centers, to an OCR audit or investigation.



Violations may result in significant fines and penalties.

These fines and penalties may be imposed for:

- Lack of appropriate administrative, technical and physical safeguards for PHI.
- Impermissible disclosures (including the failure to adhere to the minimum necessary standard).
- Failure to accommodate a patient's rights under the Privacy Rule.

Only the Privia Privacy Officer is authorized to **determine** if a **reportable breach** has occurred, and make the required notifications.

The Tier System

HIPAA enforcement penalties are organized in tiers. This tier system categorizes violations from less severe to more severe.

 Health & Human Services HIPAA Enforcement 2025 Fines		
Tier 1	No Knowledge Did not know and could not reasonably have known of the breach	\$141 - \$71,162 <i>per violation / record</i>
Tier 2	Reasonable Cause "Knew" or by exercising reasonable diligence, "would have known" of the violation, did not act with willful neglect.	\$1,424 - \$71,162 <i>per violation / record</i>
Tier 3	Willful Neglect Corrective Action Taken "Acted with willful neglect" and corrected the problem within a 30-day time period	\$14,232 - \$71,162 <i>per violation / record</i>
Tier 4	Willful Neglect No Action Taken "Acted with willful neglect" and failed to make a timely correction	\$71,162 - \$2,134,831 <i>per violation / record</i>
Source: <small>Federal Register Annual Civil Monetary Penalties Inflation Adjustment - March 17, 2022</small>		\$2,134,831 <i>Calendar Year Maximum for all Tiers</i>

Resource: <https://www.govinfo.gov/content/pkg/FR-2024-08-08/pdf/2024-17466.pdf>

What do violations look like?

Examples of Violations



- Failure to conduct a comprehensive security risk assessment
- Failure to encrypt mobile devices
- Failure to use a supported operating system with security updates
- Failure to have antivirus or anti-malware configured systems
- Failure to encrypt ePHI at rest
- Failure to use a secure email platform

Examples of OCR Enforcement

Real life examples of Office of Civil Rights (OCR) enforcement.

First Example

A solo physician practice paid \$100,000 to the OCR and adopted a corrective action plan to settle a HIPAA security rule violation. This occurred after the practice reported a breach to the OCR due to a dispute with a business associate. The OCR's investigation found that the practice had not conducted a risk analysis.



Second Example

A small rural hospital paid over \$111,000 to the OCR and adopted a substantial corrective action plan to resolve a complaint alleging that a former employee continued to have remote access to the hospital's web-based scheduling calendar, which contained PHI, after termination of employment.

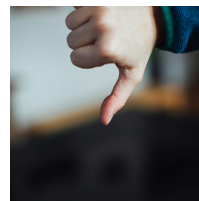
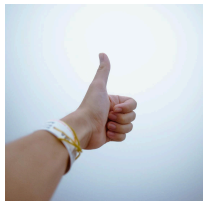


Third Example

A psychiatric medical services provider agreed to take corrective actions and pay \$28,000 to settle potential violations of the HIPAA privacy rule, including provisions of the right of access standard.



The HIPAA Privacy Rule Dos and Don'ts



When dealing with PHI **DO**:

- Only access for work-related purposes.
- Only share with authorized individuals who have a work-related need to know.
- Only follow the Minimum Necessary Rule and only disclose the minimum needed to do your job.
- Make sure all paper containing confidential information is shredded.

When dealing with PHI **DON'T**:

- Access PHI not related to your job duties (including your own chart, a colleague's chart, or a relative's/friend's chart).
- Discuss patient information except as necessary for a work-related purpose.
- Don't use actual PHI for training or testing.

Keep their information as safe as you keep your own! You are in the best position to protect the patients' privacy.

HIPAA 101: Privacy | Summary

In this lesson, we explored the crucial steps for safeguarding patient information, including understanding what constitutes Protected Health Information (PHI), implementing strong security measures, and limiting access to only authorized personnel. We also emphasized the importance of promptly reporting potential privacy incidents, following established procedures, and cooperating with investigations to protect patient privacy and maintain compliance with HIPAA Regulations.

You should now be able to:

- Identify the steps you need to take to safeguard patient information.
- Report potential privacy incidents.



Do you have questions?

Contact:

Lesley Anne M. Durant, Privacy Officer

lesleyanne.durant@priviahealth.com



The second half of this course focuses on HIPAA Security, which looks at the safeguards of protected health information stored in electronic systems. In this section of the course, you will learn about your responsibilities under the HIPAA Security Rule and how it applies to electronic protected health information or EPHI. Next, we will look at actions you can take to safeguard against cybersecurity threats, and finally, how you report a cybersecurity incident.

Learning Objectives

- Summarize the HIPAA Security Rule.
- Explain the importance of employee vigilance and reporting.
- Identify ways to report incidents.

The Security Rule



The Goal

The goal of the Security Rule is to ensure that patient information is safeguarded when it is stored in electronic systems. It applies to Covered Entities and Business Associates, and it requires us to analyze the risks computer systems present to electronic protected health information.

Security Rule

Covered entities and **business associates** must **develop and implement** reasonable and appropriate **security measures** through policies and procedures to **protect the security of ePHI** they create, receive, maintain, or transmit. Each entity must **analyze the risks to ePHI** in its environment and create solutions appropriate for its own situation.

What is “electronic Protected Health Information” (ePHI)?

ePHI is protected health information that can be found in the following formats:

- Electronic Health Record

- Spreadsheets
- Email
- Texts
- Any electronic or digital form

Responsibilities Under the Security Rule for Covered Entities and Business Associates

- Ensure the **confidentiality, integrity** and **availability** of all ePHI they **create, receive, maintain, or transmit**
- **Identify** and **protect** against reasonably anticipated **threats** to the **security** or **integrity** of the **ePHI**
- **Protect** against reasonably anticipated, **impermissible uses** or **disclosures**
- **Ensure compliance** by their workforce

ePHI Access Monitoring

ePHI Access Monitoring



Requirements

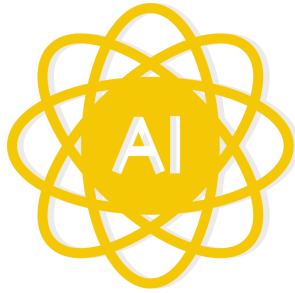


Under HIPAA, covered entities are required to monitor access to systems that contain ePHI to ensure that improper disclosure has not occurred.

“...implement mechanisms to record and **examine access** and other activity in systems that contain or use ePHI...”

[45 CFR § 164.312](#)

Artificial Intelligence



Privia uses artificial intelligence that flags potentially suspicious or anomalous activity to assist the electronic health record (EHR) auditing process.

Investigation



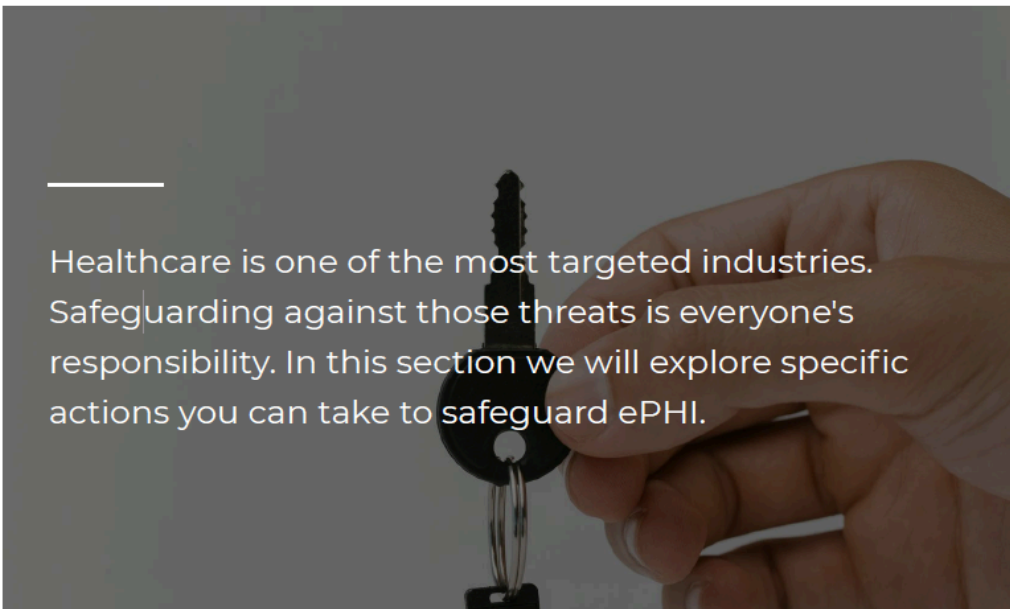
Any flag is investigated by our team of privacy experts who investigate the potential incident to determine if there was unauthorized access to PHI.

Compliance Liaison



The team may reach out to the Compliance Liaison to assist in the investigation. This will help them understand context, understand any documentation that the care center might have, and to understand any local policies and procedures.

Safeguarding Against Cybersecurity Threats

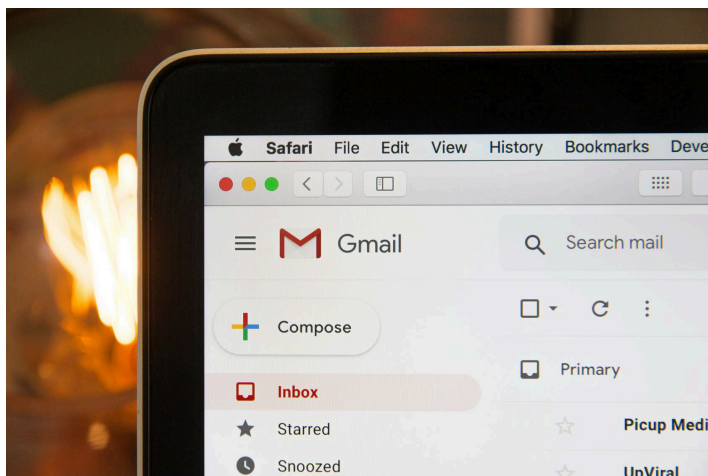


Healthcare is one of the most targeted industries. Safeguarding against those threats is everyone's responsibility. In this section we will explore specific actions you can take to safeguard ePHI.

The Top Four Threats to Healthcare Organizations

The top four threats facing healthcare are social engineering, ransomware attacks, an insider causing accidental or malicious data loss, and the loss or theft of equipment with ePHI. Below you will read about each of these threats and ways in which you can prevent security issues from happening to you.

Social Engineering



Social Engineering is an attempt to trick you into giving out personal information or infecting your device by clicking on a link to give hackers access to patient data. A common avenue for hackers is email phishing.

Social Engineering: Business Email Compromise



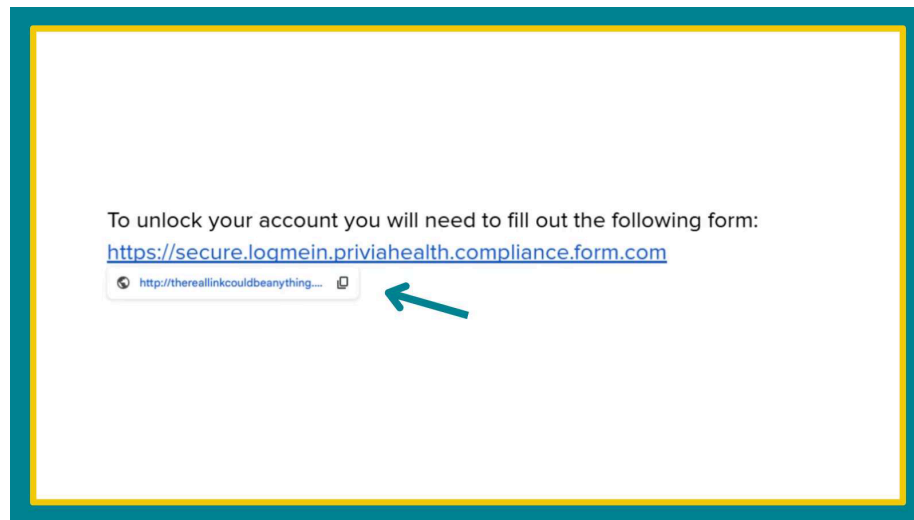
Cyber attacks against small businesses make up 71% of all attacks. Almost all start with a phishing email. Email is one of the most common ways that threat actors gain access to systems. The most common way is through a targeted phishing attack.

Cybersecurity Best Practices: Phishing

Phishing is a type of scam where someone pretends to be a trustworthy source, to trick you into sharing private info, like passwords or credit card numbers, usually through emails or messages.

Be critical of all email you receive. These steps can help protect you from becoming a victim of a phishing scam.

Best Practice: Check the "From" Address



Always check the **domain** or end of an email address to make sure it is accurate and from your organization or a known organization.

Best Practice: Verify the Link or Visit the Site Directly

To unlock your account you will need to fill out the following form:

<https://secure.logmein.priviahealth.compliance.form.com>



You can roll your over the link to verify the address or go directly to trusted sites where you login by typing it into the browser instead of following the link in the email.

Best Practice: Use Webmail

Webmail is the most secure way to view your email. Service providers release new security features and alerts in webmail first.

Best Practice: Attachments

Only open attachments you are expecting. Compressed files like .zip should never be opened unless you know the source of the email.

Best Practice: Be aware of an Unprofessional Look

Phishing emails often have telltale signs: Look for poor grammar, awkward phrasing, blurry images, misspellings, or incorrect logos. These are all red flags that indicate a scam.

Test Your Knowledge



Take Google's Free Phishing Quiz
<https://phishingquiz.withgoogle.com/>

Other Forms of Social Engineering

While phishing is the most common type of social engineering attack. Threat actors use multiple methods to get access to data.

- **Scam Callers**
 - Scam callers call pretending to be a patient or a legitimate organization. If you are in doubt call the company or patient back on their published numbers.
- **Social Media**
 - Threat actors will use information about you and your company on the internet and social media to appear legitimate.
- **SMISHING- Texting Scams**
 - Smishing is similar to phishing only using text. An attempt will be made to create an urgent situation and asking you to take action usually for financial gain like sending gift cards, money or providing a password.

BE SKEPTICAL! If something doesn't seem right, do not provide sensitive information.

Safeguarding Against Ransomware



An attack occurs when hackers gain control of data or a computer system and hold it hostage until a ransom is paid. This can put your patients in danger and prevent you from delivering care in a timely fashion.

Average Cost of Ransomware Attack



In 2024 the average cost of a ransomware attack in healthcare was \$9.77 million.

<https://www.ibm.com/reports/data-breach>

Securing Your Computer



- **Use a Company Issued Device Whenever Possible**
 - Company devices are configured to be secure & encrypted: the best way to protect our patient's information.
- **Update Your Operating System**
 - Make sure that any device you use is configured to receive automatic updates and is still supported by the manufacturer. Note: Windows 7,8, and 10 (as of October 14,2025) are no longer supported.
- **Install Antivirus Software**
 - Make sure that you have antivirus / anti-malware installed and that it is configured for automatic updates.
- **Do Not Install Unnecessary Software**
 - It is important to avoid installing unnecessary software or software from untrusted sources because doing so can expose it to potential security risks and make it easier for hackers to access sensitive information.
- **Do not use public cloud services or public AI tools to store or process ePHI**
 - You should never save ePHI in personal email (Gmail, Yahoo, AOL, Hotmail, etc.) or your personal cloud storage (One Drive, Google Drive, Dropbox, etc.) or use AI tools like ChatGPT. A Business Associate Agreement is required at all times in any location where ePHI is stored.

Cybersecurity Best Practices

Cybersecurity Best Practices: Passwords



1. Never Share Your Password

Your username and password are unique to you and should never be shared with another individual. You should never provide your current password in a link you clicked from an email.

2. If asked for your password, BEWARE!

If a caller, text message, or email link asks you to enter a password, it is likely an attempt to steal your password! Never share your password!

3. Upgrade to a passphrase

Passphrases are easier to remember and are more secure due to length.

For example: I love passwords! - 17 characters and complex, but easy to remember.

4. Use Multifactor Authentication (MFA)

Whenever possible, configure MFA to prevent password theft; it adds an extra layer of protection to your accounts by requiring more than just a password.

5. Always lock your computer

Always lock your computer when you walk away to prevent someone from taking unauthorized actions under your account, especially in patient charts.

6. Do not save your password

Do not check the remember password box or save your password in your browser. Especially on shared computers, use a password manager instead.

Safeguarding Against: Insider, Accidental or Malicious Data Loss



Insider threats are a serious risk. They may involve people in your organization, employees, contractors, or other users who have legitimate access to your computer systems and network. It could be simple human error, negligence, or malice that cause insiders to compromise patient data.

ePHI Access Monitoring



Privia uses artificial intelligence that flags potentially suspicious or anomalous activity to assist the electronic health record (EHR) auditing process.

Each potential incident is investigated by Privia's Privacy Team to ensure an improper disclosure did not occur.

[45 CFR § 164.312](#)

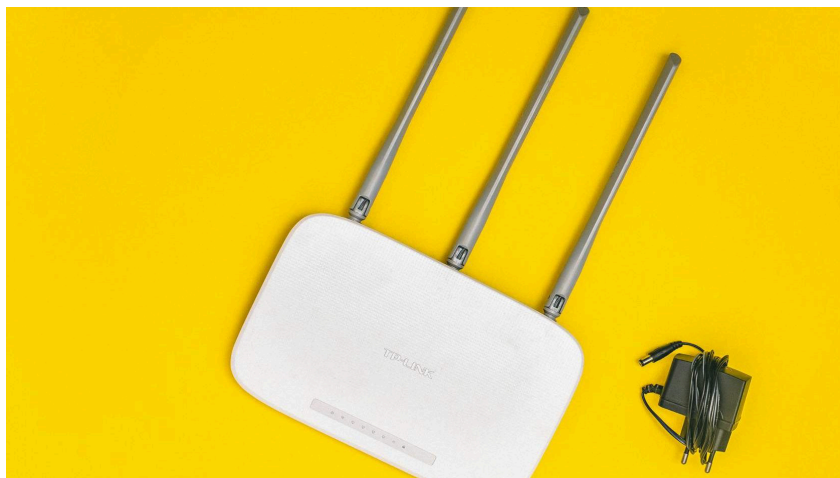
Working Outside the Office: Best Practices

Cybersecurity Best Practices: Working Outside the Office



1. Try to work in a private area. This helps keep private information safe from others.
2. Avoid discussing patients' health information in public places where someone might overhear. Always take calls in private when discussing this information.
3. Don't leave any health information unattended. Make sure your computer is locked if you step away. Don't leave any papers with sensitive information where others can see them.
4. Be careful if you share your computer with others in your home. They might accidentally see private information or install software that could be a security risk.
5. Don't save or print patients' health information on your home computer. Keep this info in the official records system. You shouldn't save this info in personal cloud storage like Google Drive or Dropbox. Try not to print these documents, but if you have to, shred them when you're done. This helps keep our patients' information safe.

Home Router / WiFi



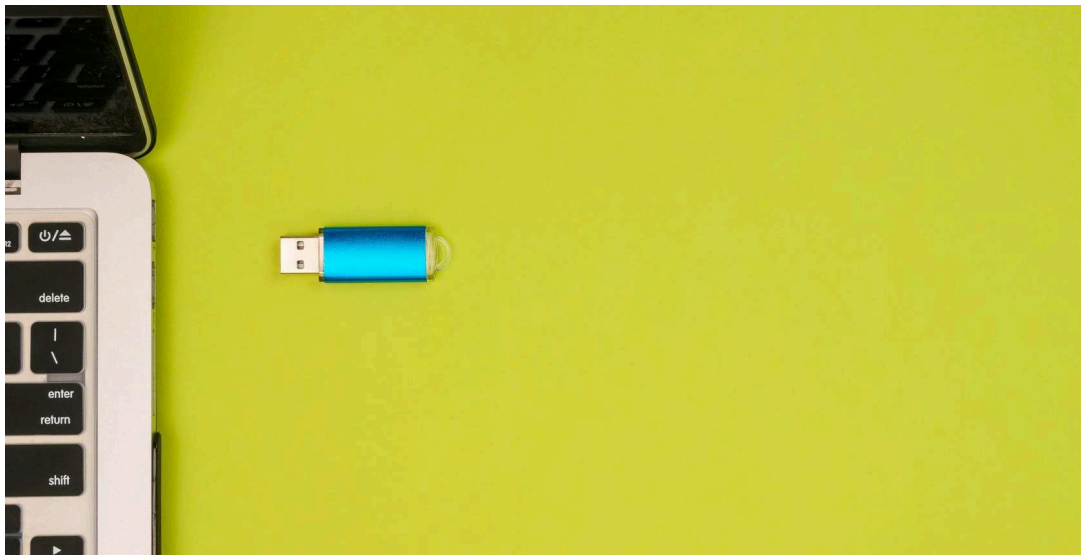
1. Keep your router updated. Always use the latest firmware, and set it up to update automatically.
2. Change the default password on your router. This makes it harder for unwanted visitors to get into your Wi-Fi or threat actors installing malware on your network.
3. Secure your wireless connections. Change the name and password that came with your router. Use WPA2 for your security protocol since it's the most secure, and turn off WPS.
4. You can also set up a guest network. This lets visitors use your Wi-Fi without having access to your personal or work devices.

Resources

How to Make Your WiFi as Secure as Possible: <https://rb.gy/jxfsnc>

Secure Your Home Network: <https://rb.gy/eeq6bt>

Safeguarding Against Loss or Theft



Everyday devices such as laptops, smartphones, and USB/thumb drives are often lost or stolen and could end up in the hands of hackers or lead to improper disclosure.

Encryption and Proper Disposal of Media



1. Always use encryption!

Any device storing patient information, such as flash drives, phones, or tablets, should be encrypted. Without it, any data on the device is assumed to be a breach if lost or stolen.

2. Proper Disposal

You can't just throw a device that contains ePHI in the trash or recycle it. You need to safely destroy that information. Use a service that gives you a disposal certificate.

3. Maintain and Inventory

Keep track of all devices that are destroyed. We are required to keep an inventory and disposal certificates for seven years.

4. Hard Drives and Flash Drives

Remove and securely wipe, shred, or destroy them before disposing of a device. Record the serial number and how it was destroyed.

Reporting Incidents

Any privacy, security incident, or suspected breach of PHI must be reported to Privia within three business days.

Faster reporting typically leads to better investigation outcomes and mitigation.

Not ALL Incidents are the same. Review each card to see how to report the information on the card.

**Lost a device with
patient information?**

Let your manager, Care Center's Compliance Liaison, or Privacy Officer know right away if you lost a device with patient information.

**Need to reset a
password, think you
have a virus?**

Call the Privia Technology Service Desk for technical remediation and investigation of virus, malware, phishing, username/password etc.
888.774.8428 option 1.

Getting Spam in your inbox?

Use your email system's tools. If you think information may have been compromised contact Privia's Privacy Officer or IT.

Cybersecurity Incidents



Report cybersecurity incidents right away by visiting our website at compliance.priviahealth.com or email compliance@priviahealth.com.

Checklist

- ☐ Be critical of email, texts and calls - if it feels like a scam, it probably is.
- ☐ Use passphrases and do not share your password with anyone.
- ☐ Always use a secure work device and never share a computer with others that you use to access ePHI.
- ☐ Always dispose of devices that contain ePHI securely.
- ☐ If you suspect a breach, notify Privia's Compliance, Privacy, and Cybersecurity team immediately by visiting compliance.priviahealth.com or emailing: compliance@priviahealth.com.
- ☐ You are the secret to securing our patients' data!

Course Summary

You should now be able to:

- Summarize the HIPAA Privacy and Security Rules.
- Identify the steps you need to take to safeguard patient information.
- Explain the importance of employee vigilance and reporting.
- Report potential privacy incidents.



Questions?

Contact

Lesley Anne M. Durant, Privacy Officer

lesleyanne.durant@priviahealth.com

or

Paul Shenenberger, Chief Information Security Officer

paul.shenenberger@priviahealth.com