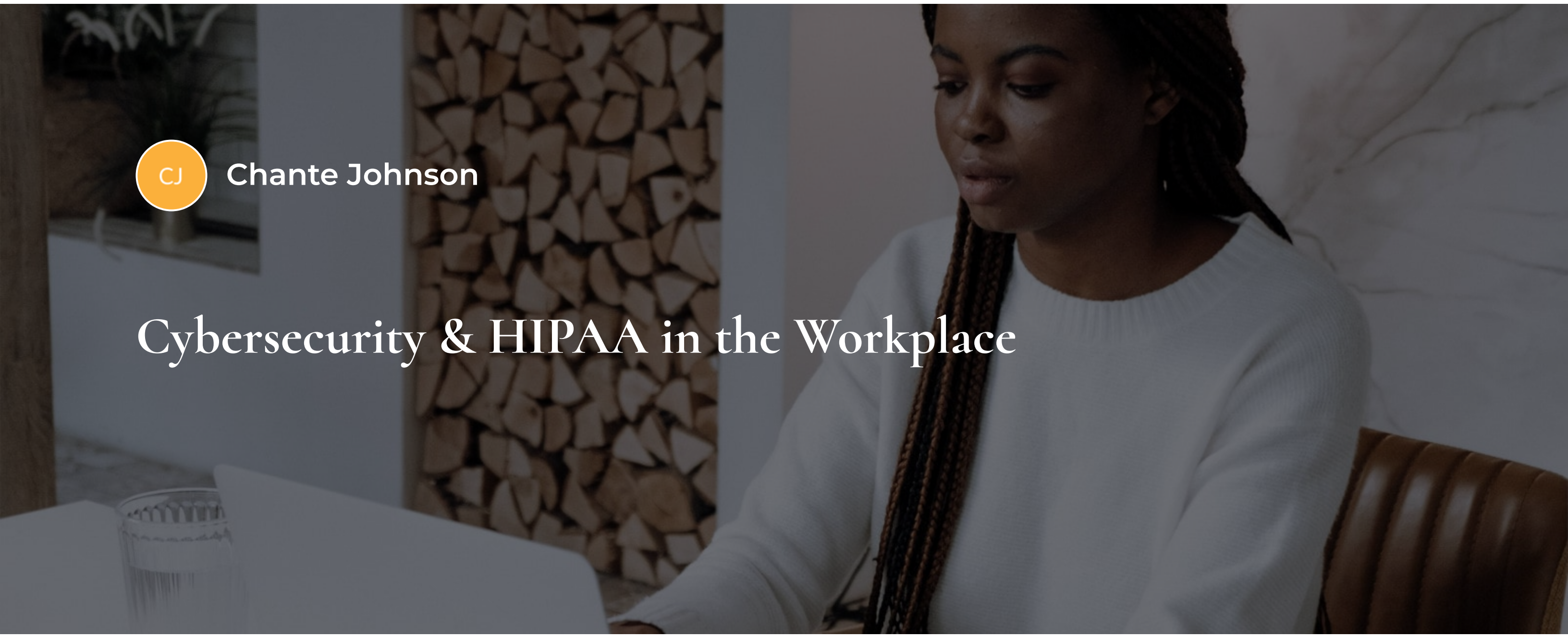


CJ Chante Johnson

Cybersecurity & HIPAA in the Workplace

Lesson 1: Protecting Data Starts with You

“Security is not a product, but a process.” – Bruce Schneier

In today’s digital workplace, safeguarding sensitive information isn’t just an IT responsibility—it’s part of everyone’s job. Whether you're handling patient records, sending emails, or accessing files remotely, your actions impact data security and HIPAA compliance.

This module will help you:

- Recognize common cybersecurity threats
- Understand what HIPAA requires in everyday work
- Build habits that protect your organization and the people it serves

Let’s get started—one quick lesson at a time.

▶ 0:47 1x

Your Role in Protecting Sensitive Information

Every day, employees interact with data that must be protected—whether it's a patient’s medical history, a colleague’s personal details, or confidential business files. Cybersecurity and HIPAA compliance aren’t just policies—they’re part of how we build trust, protect privacy, and avoid costly breaches.

This lesson explores:

- What counts as sensitive data
- Why HIPAA applies to more than just healthcare workers
- How simple actions can prevent serious consequences

▶ 0:39 1x

"What Is Protected Health Information (PHI)?"

- Name
- Date of birth
- Medical record number
- Email address
- Health conditions
- Insurance details

▶ 0:19 1x

Which of the following is considered PHI?

○ A patient’s email address

○ A list of medications

○ A birthdate

○ All of the above

SUBMIT

Lesson 2: Cybersecurity Basic

Cybersecurity isn’t just about firewalls and IT teams—it’s about the everyday choices you make. From the passwords you create to the emails you open, your actions help prevent data breaches and protect patient privacy.

In this lesson, you’ll learn:

- How to spot suspicious activity
- What makes a strong password
- Why software updates matter
- How to secure your devices and workspace

▶ 0:37 1x

Cybersecurity Essential

Section 1: Strong Passwords & MFA

- Use at least 12 characters
- Mix letters, numbers, and symbols
- Enable multi-factor authentication (MFA) whenever possible

Section 2: Recognizing Phishing Attempts

- Look for misspellings, urgent language, and unfamiliar senders
- Never click unknown links or download unexpected attachments
- Report suspicious emails to IT

Section 3: Device Security

- Keep software and antivirus programs up to date
- Lock your screen when stepping away
- Avoid public Wi-Fi for sensitive tasks

▶ 0:44 1x

You receive an email from “IT Support” asking you to reset your password immediately. The link looks odd, and the sender’s address ends in “.net.” What should you do?

○ Click the link and reset your password

○ Forward the email to your manager

○ Report it to IT and delete the message

SUBMIT

Which of the following is a good cybersecurity habit?

○ Writing your password on a sticky note

○ Using MFA for login

○ Ignoring software updates

SUBMIT

Lesson 3: HIPAA Essentials

Understanding HIPAA in the Workplace

The Health Insurance Portability and Accountability Act (HIPAA) protects sensitive health information and sets rules for how it's handled. Whether you work in healthcare, HR, IT, or admin support, HIPAA affects how you manage data.

This lesson covers:

- What qualifies as Protected Health Information (PHI)
- Who must follow HIPAA rules
- The "minimum necessary" standard
- Real-world examples of compliance

▶ ● 0:40 1x

HIPAA at a Glance

- 1996: HIPAA enacted to protect health data
- 2003: Privacy Rule implemented
- 2009: HITECH Act strengthens enforcement
- 2013: Omnibus Rule expands responsibilities
- Today: HIPAA applies to digital and cloud-based environments

▶ 0:24 1x

Key Concepts

▶ 0:01 1x

Covered Entities

▶ 1x

Healthcare providers, health plans, and clearinghouses

▶ 1x

Business Associates

1x

Vendors or contractors who handle PHI on behalf of covered entities

1x

PHI Examples

1x

Names, birthdates, medical records, insurance info, email addresses

1x

Minimum Necessary Rule

1x

Only access the data you need to do your job—no more, no less

1x

You're helping onboard a new employee and see a spreadsheet with names, birthdates, and medical conditions. Is this PHI?

○ No, it's just HR data

○ Yes, it contains identifiable health information

SUBMIT

Who must comply with HIPAA regulations?

○ Only doctors and nurses

○ Anyone who handles PHI

○ Only IT staff

SUBMIT

Lesson 4: Everyday Risks at Work

Small Mistakes, Big Consequences

Even with strong policies in place, everyday habits can expose sensitive data. Whether you're working from home, chatting in the hallway, or printing documents, it's easy to overlook risks. This lesson helps you spot and prevent common workplace slip-ups.

You'll learn:

- How physical spaces and digital habits affect data security
- What to avoid when working remotely
- How to protect PHI in shared environments

▶ ● 0:38 1x

Risk Hotspots in the Office

“Where Data Can Leak”

- Unlocked workstation
- Printed documents left on the copier
- Conversations in public areas
- Sticky notes with passwords
- Unattended mobile devices

0:18 1x

Remote Work Risk

“Where Data Can Leak”

- Unlocked workstation
- Printed documents left on the copier
- Conversations in public areas
- Sticky notes with passwords
- Unattended mobile devices

Secure Habits for Daily Tasks

- Lock your screen when stepping away
- Shred printed documents with PHI
- Avoid discussing sensitive info in public
- Use encrypted platforms for communication
- Keep mobile devices password-protected

Which of the following is a HIPAA violation?

□ Leaving a patient file on your desk overnight

□ Discussing a diagnosis in a crowded elevator

□ Using a personal email to send PHI

SUBMIT

Lesson 5: Sharing Data Safely

Think Before You Send

Sharing information is part of everyday work—but when it involves sensitive data, you need to be intentional. Whether you're emailing a file, uploading to the cloud, or chatting in Teams, it's your responsibility to protect what you share.

This lesson covers:

- Safe email practices
- Secure file sharing tools
- Verifying recipients before sending
- What to do if you send something by mistake

▶ 0:38 1x

Secure Sharing Methods

▶ 0:02 1x

Email Encryption

▶ 1x

Use built-in encryption tools in Outlook or Gmail. Add “[Secure]” to the subject line if required by your organization.

▶ 1x

Business Associates

Vendors or contractors who handle PHI on behalf of covered entities

Verifying Recipients

Double-check email addresses before sending. Use distribution lists carefully. Never assume autofill got it right.

You accidentally emailed a patient’s file to the wrong coworker. What should you do?

○ Ask the coworker to delete it and move on

○ Notify your supervisor and follow breach protocol

○ Try to recall the email and hope no one saw it

SUBMIT

Tool & Task Quick Reference

Tap each card to reveal how different platforms support (or compromise) data security and HIPAA compliance.

▶ 0:11 1x

Outlook with encryption

▶ 1x

Use Outlook with encryption to send sensitive information securely, such as PHI, ensuring compliance with data protection policies.

▶ 1x

SharePoint folder

1x

A SharePoint folder is ideal for team collaboration, allowing secure file sharing and version control within an organization.

1x

Teams chat

1x

Teams chat is perfect for quick team communication but avoid sharing sensitive or confidential information in this platform.

1x

Personal Dropbox

1x

Avoid using personal Dropbox accounts for storing or sharing sensitive data, as they may lack necessary security measures.

1x

Share PHI securely

1x

To share PHI securely, use tools like Outlook with encryption or approved secure file-sharing platforms.

1x

Collaborate with team

1x

For team collaboration, use tools like SharePoint or Teams, ensuring secure and efficient communication and file sharing.

1x

Which of the following is a secure way to share PHI?

○ Personal email

○ OneDrive with restricted access

○ Public Google Drive link

SUBMIT

Lesson 6: Breach Response

What to Do When Things Go Wrong

Even with strong habits and secure tools, mistakes happen. A breach doesn't always mean a hacker—it could be an accidental email, a lost device, or a conversation overheard in public. The key is knowing what to do next.

This lesson covers:

- What counts as a breach
- How to respond quickly and responsibly
- Internal reporting protocols
- Why timing matters

Responding to a Suspected Breach

Step 1: Identify the incident (e.g., misdirected email, lost laptop, overheard PHI)

Step 2: Notify your supervisor or compliance officer immediately

Step 3: Document what happened and who was affected

Step 4: Follow internal protocols for containment and reporting

Step 5: Cooperate with any investigation or follow-up actions

You overhear a coworker discussing a patient's diagnosis in the break room. What should you do?

□ Ignore it—it wasn't your conversation

□ Gently remind them that PHI should be discussed privately

□ Report it to your supervisor or compliance officer

SUBMIT

Common Breach Examples

- Sending PHI to the wrong recipient
- Leaving printed records in public areas
- Discussing patient info in hallways or elevators
- Using unsecured devices to access sensitive data

▶ 0:19 1x

You're uploading a spreadsheet with PHI to a Teams channel. The channel includes external collaborators. What should you do?

○ Try to fix it yourself

○ Notify your supervisor or compliance officer

○ Delete the evidence

SUBMIT

Lesson 7: Cybersecurity & HIPAA in the Cloud

Working Securely in the Cloud

Cloud platforms make it easy to collaborate, share files, and access data from anywhere—but they also introduce new risks. HIPAA compliance doesn't stop at the desktop. Whether you're using OneDrive, SharePoint, or Teams, it's essential to understand how to protect sensitive information in cloud environments.

This lesson covers:

- How cloud tools support HIPAA compliance
- Best practices for access control and sharing
- What to avoid when working in shared spaces
- How to use audit trails and version history

▶ 0:44 1x

Cloud Security Essentials

Section 1: Access Controls

- Use role-based permissions
- Limit access to PHI based on job function
- Avoid "Everyone" or "Public" sharing settings

Section 2: Audit Trails & Version History

- Track who accessed or edited a file

- Restore previous versions if needed
- Use logs to investigate potential breaches

Section 3: Data Retention & Storage

- Follow organizational policies for retention
- Avoid storing PHI in personal cloud accounts
- Use encrypted storage options when available

▶ ● 0:42 1x

Which of the following is a secure cloud practice?

○ Sharing PHI via a public Google Drive link

○ Using OneDrive with restricted access

○ Uploading PHI to a personal Dropbox

SUBMIT

Lesson 8: Final Assessment & Certificate

Show What You Know

You’ve explored the essentials of cybersecurity and HIPAA—from everyday risks to cloud collaboration. Now it’s time to test your knowledge and earn your certificate of completion.

This final quiz covers:

- PHI identification
- Secure sharing practices
- Breach response steps
- Cloud security and compliance

▶ 0:28 1x

Which of the following is considered PHI?

○ A patient’s name

○ A birthdate

○ A medical record number

○ All of the above

SUBMIT

What’s the first step if you suspect a data breach?

○ Try to fix it yourself

○ Notify your supervisor or compliance officer

○ Delete the evidence

○

SUBMIT

Which platform is best for securely sharing PHI?

○ Personal Dropbox

○ OneDrive with restricted access

○ Public Google Drive

○

SUBMIT

Statement of Completion

🎉Congratulations! You’ve completed the Cybersecurity & HIPAA in the Workplace module.

You’ve earned your certificate and demonstrated your commitment to protecting sensitive data.

You can link to a downloadable certificate or badge if your LMS supports it, or simply mark the course as complete.

▶ 0:21 1x

1. **Always back up your files.** When malware erases files from your device or network, those files are often unrecoverable. So, keep your most important files backed up on an external drive and store them in the cloud.

2. **Keep software up to date.** Does your computer notify you when you need a software update? As cumbersome as they may seem, updates protect against potential security breaches by addressing vulnerabilities. The next time you get a notification, install the update.

3. **Install antivirus software.** Get antivirus software that automatically looks for trouble in the background. Think of it like installing a security alarm at your house–it alerts you when there

are intruders in the system. *Note: This is not a fail-safe and can't always detect all threats.*

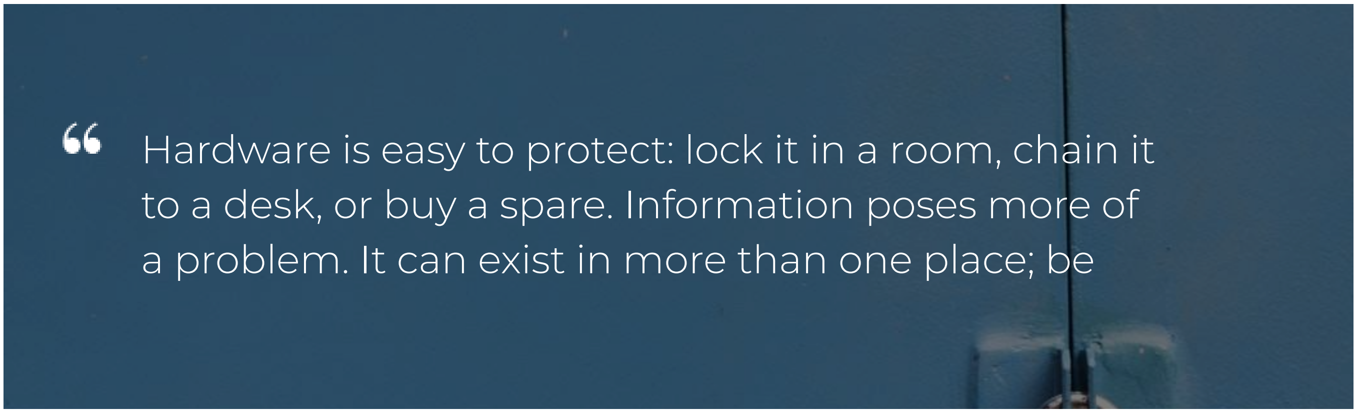
4. **Use strong passwords.** Predictable words and sequences make the worst passwords because hackers can easily run countless word and number combinations to crack your account. Use long passwords that contain letters, numbers, and symbols.

5. **Enable MFA.** Multifactor authentication (MFA) allows you to protect your data through various layers. Instead of merely protecting your account with a password, you also obtain verification through phone or email. So, even if someone obtains your password, they still won't be able to access the account without also having access to your phone or email.

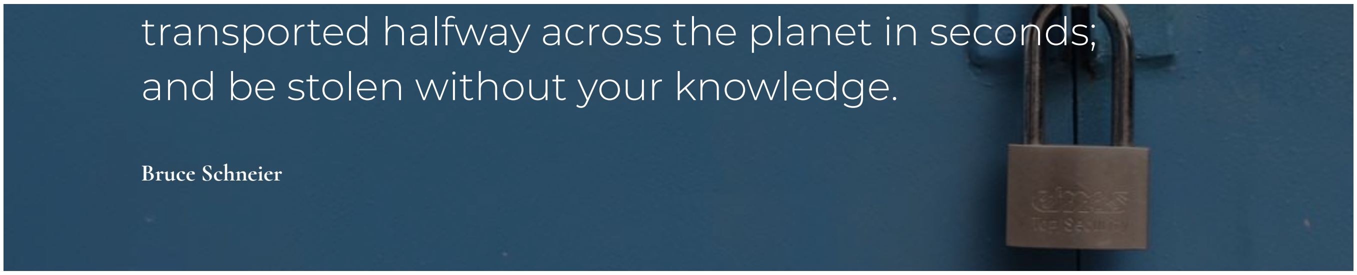
6. **Beware of unknown senders.** Never open email file attachments sent by someone you don't know. Sometimes, the email will seem like it's from an acquaintance—a method known as *spear-phishing*. So, before opening a file, always double-check the sender's email address.

7. **Check URLs.** One of the easiest ways to know if you're entering a safe website is to check the URL. Today, secure websites all use a URL that starts with *https*. If you see that a website URL starts with *http*, it's not a secure place to conduct sensitive activity.

▶ 2:24 1x



> “Hardware is easy to protect: lock it in a room, chain it to a desk, or buy a spare. Information poses more of a problem. It can exist in more than one place; be



> transported halfway across the planet in seconds; and be stolen without your knowledge.
>
> Bruce Schneier

Summary

Cybersecurity and HIPAA compliance aren’t one-time tasks—they’re part of your everyday workflow. Whether you need help, want to refresh your knowledge, or are looking for tools to stay sharp, these resources are here for you. To prevent security breaches, remember these seven key tips:

1. Always back up your files.
2. Keep software up to date.
3. Lock your screen when stepping away
4. Use encrypted platforms for PHI.
5. Report suspected breaches immediately.
6. Avoid public Wi-Fi for sensitive tasks.
7. Double-check recipients before sharing files.

You’ve built a strong foundation in protecting sensitive data. Keep practicing, stay alert, and lead by example. Security isn’t just a policy—it’s a mindset.

▶ 0:55 1x

Small steps can make a world of difference. It may seem daunting to address hacking and security breaches, but these small steps can often save you from big trouble down the road. In most cases, thieves will target a house with a single, easy-to-break lock rather than a home with multiple levels of security.

▶ ● 0:20 1x