

# Compliance

## 2025 HIPAA 201 | Privacy and Security for Privia Business Associates

# Training

☰ Course Instructions

☰ Introduction

HIPAA

---

☰ Learning Objectives

☰ HIPAA

☰ To Whom Does HIPAA Apply?

APPLY THE PRIVACY RULE AS A PRIVIA BUSINESS ASSOCIATES

---


☰ Compliance Liaison

☰ Validating the Care Center Roster

 **Annual Compliance Training** **Policy Awareness and Sanctions: Building a Culture of Compliance** **ePHI Access Monitoring** **Collaborate on User Audits** **Breach Notification**


#### MANAGING YOUR BUSINESS ASSOCIATES

---

 **What is a Business Associate?** **Business Associate Agreements** **Third Party Access Review**

#### APPLYING THE SECURITY RULE AS A PRIVIA BUSINESS ASSOCIATE

---

 **Security Policies** **Security Risk Assessment Attestation** **Workforce Authorization**

#### SAFEGUARDING YOUR CARE CENTER

---

 **HIPAA Enforcement Rule** **Cyber Liability Insurance** **Technical Controls & Managed Security Services: Protecting Your Care Center's Digital Frontline**

#### COMPLIANCE, PRIVACY, AND SECURITY- TOOLS AND CHECKLISTS

---

 **Calendar & Timelines**

 **Privacy & Security Checklist**

**COURSE SUMMARY AND KNOWLEDGE CHECK**

---

 **Course Summary**

 **What's Next?**

# Course Instructions

## Instructions:

1. Throughout this course you will find interactivity and embedded questions.
2. You may need to complete some activities before you are able to progress through the course.
3. At the end of the course you will have a knowledge check.
  - a. You can return to the course material to answer these questions.
  - b. You must score an 80% or better to get credit for the course.
4. There is audio throughout the course, please have your headset or speakers available.
5. Select continue to begin the course.

CONTINUE





**Embedded Links:** Links in this training will launch in a new tab. Please be sure to return to the Privia University tab to continue with your training after launching any links.

## Welcome to the HIPAA Privacy & Security Annual Training

Welcome to HIPAA 201 | Privacy and Security for Business Associates. This course is designed to provide Privia Business Associates with information regarding the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the steps employees must take to safeguard protected health information and report privacy or security concerns.

CONTINUE

# Welcome to HIPAA 201 Training



## Learning Objectives:

**By the end of this module you will be able to:**

- Protect patient privacy and safeguard PHI with the appropriate controls.
- Provide patients access to their records in a timely manner.
- Reduce the risk of regulatory, reputational, and cybersecurity events.
- Provide Care Centers with tools to assist them with their Privacy & Security Programs.
- Comply with all contractual obligations of our public and private payers.
- Ensure compliance with all applicable laws and regulations.

CONTINUE

# HIPAA

## What is the Health Insurance Portability and Accountability Act (HIPAA)?

**HIPAA** is a federal law that sets a minimum standard for how patient information must be protected.

CONTINUE

## History and Purpose of HIPAA

We frequently look at HIPAA as a single regulation, but HIPAA is a series of regulations passed and amended over the years. Take a look at the timeline below and what each addition to the rule added.

2003

### Privacy Rule

The privacy rule controls how we disclose patient information, how we protect patients' privacy, and how they gain access to their records.

2005

### **Security Rule**

The security rule outlines the technical, administrative, and physical controls that we need to put in place to safeguard ePHI.

2006

### **Enforcement Rule**

The enforcement rule allows Health and Human Services (HHS) to enforce all the provisions of HIPAA and level fines.

2009

### **Breach Notification**

The breach notification rule outlines what covered entities have to do in the event of a breach.

2009-2013

### **Business Associates (HITECH & Omnibus Rule)**

The Health Information Technology for Economic and Clinical Health (HITECH) Act and the Omnibus Rule changed how business associates were treated under HIPAA. It requires Business Associates to comply with the Privacy & Security Rule and to be held individually liable.

**CONTINUE**

# To Whom Does HIPAA Apply?



## 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 that require, or involve the use or disclosure of protected health information on behalf of, or provides services to, a HIPAA Covered Entity.

[HHS defines Business Associates](#)



CONTINUE



## Covered Entity or Business Associate?

Flip each card below to see how HIPAA identifies the areas below:

Privia Medical Group

Privia Medical Group is  
a **Covered Entity**.

Privia Care Center

Your Care Center is a  
**Business Associate** of Privia  
Medical Group. In some  
instances, your Care Center  
may also be a Covered Entity  
as well.

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.



Complete the content above before moving on.

# Implementing the HIPAA Privacy Rule: Your Role as a Privia Business Associate

## Compliance Liaison



Each Privia Care Center is required\* to designate a Compliance Liaison, who:

- Serves as the primary contact for compliance, privacy, and security initiatives.
- Assists Privia in executing, tracking, and following up on these initiatives.
- Is authorized to make decisions on behalf of the Care Center.
- Is often the office manager, but can be another designated individual.
- Ensures staff is proficient in identity verification.

## COMPLIANCE LIAISON RESPONSIBILITIES



**If you need to update your Compliance Liaison, you can always contact your Operations Consultant or you can update the liaison as part of the Annual Security, Privacy, and Compliance Attestation.**

CONTINUE

## Validating the Care Center Roster



### Roster Validation

**Validating the Care Center Roster** is one of the responsibilities of the Compliance Liaison.

Let's explore a little more about that now.

CONTINUE

## What is a Care Center Roster?

The Care Center roster is all of the individuals who are authorized to access PHI on the Care Center's behalf. Individuals not on the roster may lose access to Privia systems after the Compliance Liaison and Privia Connect admin(s) for the Care Center are notified.

### Workforce Members —

Workforce members include employees, volunteers, trainees, or anyone under the direct control of your care center. These individuals may work full-time, part-time, permanently, or temporarily, regardless of whether they are paid or by whom they are paid.

Examples of workforce members include:

- Care center employees
- Temporary or agency staff
- 1099 contractors.

It is important to ensure that all workforce members are properly validated and accounted for in the care center roster.

### Non-Workforce Members —

Non-workforce members are typically third parties over whom the care center does not have direct control. These individuals or entities perform work on behalf of the care center but are not directly managed by it.

Examples of non-workforce members include:

- Hospitalist
- Phlebotomists employed by an outside lab
- Third-party accountants or bookkeepers
- Medical students

- Clinical support vendors

Properly distinguishing non-workforce members from workforce members is essential for maintaining an accurate and compliant Care Center roster.



**The primary difference between workforce and non-workforce members is that workforce members are required to complete annual compliance training.**

### **Each team member's record includes:**

- Name and date of birth
- Role and specialty for providers
- Level of access required
- Email address & contact information

**All added team members must pass an Office of the Inspector General Exclusion check.**



## Leaves of Absence

It's important to notify Privia of anyone who is on a leave of absence. A leave of absence delays requirements around the reporting for compliance training and allows us to suspend those accounts, so inappropriate access doesn't occur.

For any workforce member on a leave of absence, you are required to submit a case, and we will work with you to suspend the user's access and exclude them from our compliance training escalation procedures until they return to work.

## Resource

*This resource is on Privia Connect and will require your Privia Connect login to view.*

**Add a New Team Member or Provider | Privia Connect**



LINK

CONTINUE

## Annual Compliance Training



### Annual Compliance Training

**Why:** We are required by HIPAA, our public and private payers, and state and local laws to complete certain trainings on an annual basis.

**Who:** Any individual who is on a care center's roster as a workforce member is required to complete annual compliance training.

**When:** Annually

The Compliance Liaison is vital to the successful completion of **annual compliance training** every year. Their responsibilities include:

- Facilitating Annual Compliance Training

- Ensuring Roster is verified before training starts
- Submitting any leave of absences
- Running reports on Privia University to monitor training progress
- Following up on incomplete training assignments
- Ensuring all workforce members complete training prior to the due date\*

\*Individuals who do not complete Compliance Training timely may lose access to Privia systems after the Compliance Liaison and Privia Connect admin(s) for the Care Center are notified

[45 CFR §164.530 \(b\)](#)

CONTINUE

## Policy Awareness and Sanctions: Building a Culture of Compliance



### Policy Awareness and Sanctions

Protecting patient privacy and security is a shared responsibility. Understanding and adhering to established policies is crucial to maintaining the highest standards of care.

#### **The Foundation of Our Compliance Program**

Our compliance program is built on policies adopted by the Privia Medical Group's Board of Directors. These policies outline the minimum requirements the medical group and each care center must comply with to ensure we meet regulatory and contractual obligations. All policies can be found on Privia's policy management platform, linked on Privia Connect.

#### **Tools for Your Success: Privia's Support Resources**

Privia provides resources to help care centers build and maintain their privacy and security programs:

- **Posters:** Display these in your care center to raise awareness about compliance.
- **Newsletter Updates:** Stay informed about new policies, regulations, and potential threats.
- **HIPAA Policy Blueprints:** Utilize these templates on Privia Connect to develop your care center's own privacy and security program.

### **Maintaining Accountability: The Role of Sanctions**

Sanctions play a crucial role in maintaining compliance. They are enforced when necessary to address policy violations and ensure everyone is upholding the highest standards for patient data protection. The specific sanctions process is outlined in the relevant policies, available on Privia's policy management platform.

By working together to understand and follow our policies, we create a secure environment for our patients and build trust in our practice.



**All members of the Privia Affiliated Covered Entity (ACE) and/or Organized Healthcare Arrangement (OHCA) are required to comply with all policies adopted by the applicable Privia Medical Group or Privia Quality Network Board of Directors.**

**CONTINUE**

## ePHI Access Monitoring

**Click 'START' to explore more about ePHI access monitoring.**

## ePHI Access Monitoring



## Requirements



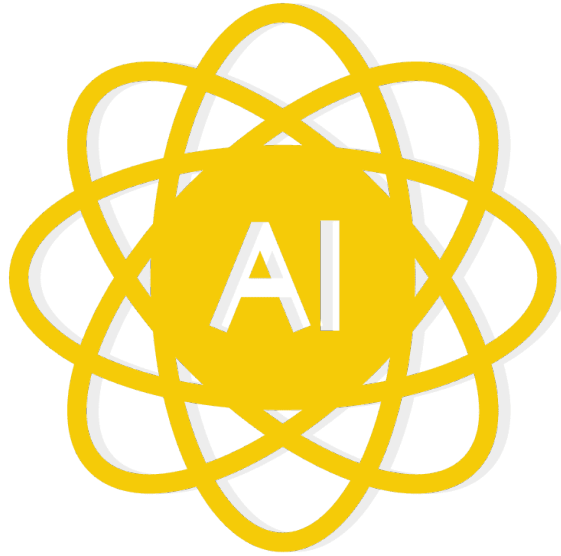
Under HIPAA, covered entities are required to monitor access to systems that contain ePHI to ensure that improper disclosure has not occurred.

“...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

### COMPLIANCE LIAISON RESPONSIBILITIES

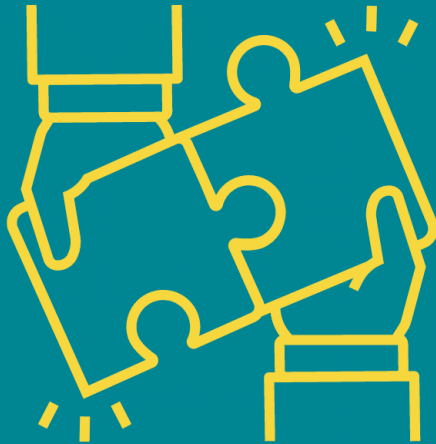


The team may reach out to the Compliance Liaison to assist in the investigation. This will help them understand context, understand any documentation that the care center might have, and to understand any local policies and procedures.



Complete the content above before moving on.

## Collaborate on User Audits



### Collaborate on User Audits

**The Compliance Liaison is also required to collaborate on user audits by doing the following:**

- Provide background documentation requested by the Privacy team.
- Enact sanctions if required.

Anyone who acts with malicious intent to criminally share PHI will permanently lose access to Privia systems.

CONTINUE

# Breach Notification

## What is a Breach?

A breach is an impermissible use or disclosure, unless there is a low probability that the PHI has been compromised, based on a four part risk assessment conducted by Privia's Privacy Officer.

## If Privia's Privacy Officer determines there has been a breach, you must notify:

- The affected individuals less than 60 days after a breach is discovered
- HHS immediately for breaches of 500+ individuals
- The media for breaches of 500+ individuals



**An annual report is sent to HHS of all breaches, including breaches of less than 500 individuals.**

**Click 'START' below to learn about how to report an incident of a suspected breach.**

## Reporting an Incident of a Suspected Breach



## Three Business Days



Any privacy issues, security incidents, or suspected breaches of PHI must be reported to Privia within three business days.

**Faster reporting typically leads to better investigation outcomes and mitigation.**

## How to Report



If you suspect a breach or need to report an incident then visit [compliance.priviahealth.com](https://compliance.priviahealth.com).

### **What to include:**

- Date / Time of Incident
- Details of the event including the systems involved
- Best contact phone for the investigation team to call



## Follow-Up



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

CONTINUE

# Managing Your Business Associates



## **What is a business associate?**

A business associate is someone or a company that does work or provides a service for your care center and needs access to PHI.

In this section we're going to look at the importance that business associates play within your care center, and the appropriate actions you need to take to manage them successfully. As part of the HITECH Act and the Omnibus Rule, HHS clarified the responsibility and accountability of business associates to comply with the HIPAA Privacy and Security Rule and that they would be accountable for any violation.

CONTINUE

## Who are Business Associates?

A **business associate** is an individual or a company that **does work** or **provides a service** for your care center and **needs access to PHI**.

Any vendor who **creates, receives, maintains, or transmits PHI** while **performing services on behalf of your care center** is a **business associate**.

CONTINUE

### Examples of Possible Business Associates:

- Practice management services
- Billing companies
- Answering services
- Scribe services
- Medical transcriptionists
- Translator services
- Shredding services
- Information technology vendors
- Cloud vendors
- IT consultants

## CONTINUE

If you need help determining if a company or individual is a business associate, you can ask yourself some questions to help decide who qualifies as a business associate. Read the questions below and flip the cards to see the answers.

**Is the person or entity doing work for your care center, or are they working for themselves or directly for the patient?**

If a person or entity is doing work for themselves or directly for the patient, they **ARE NOT YOUR BUSINESS ASSOCIATE.**

**Is the person or entity performing a function or providing a service that requires use or access to PHI on behalf of my Care Center?**

If the person or entity is performing a function or providing a service that requires use or access to PHI on behalf of your Care Center, they **ARE YOUR BUSINESS ASSOCIATE.**

**Is the person or entity performing a function or providing a service an employee of my Care Center?**

If the person or entity performing a function or providing a service is an employee of your Care Center, they **ARE NOT YOUR BUSINESS ASSOCIATE.**



Complete the content above before moving on.

## HIPAA Conduit Exception Rule\*

If a vendor transmits PHI or ePHI and does not have access to the transmitted information, and does not store copies of the data they are **not a business associate**.

\*Very narrow exception

### Examples of Conduits

- ✓ United States Postal Service
- ✓ FedEx, UPS, DHL
- ✓ Phone Company
- ✓ Internet Service Provider

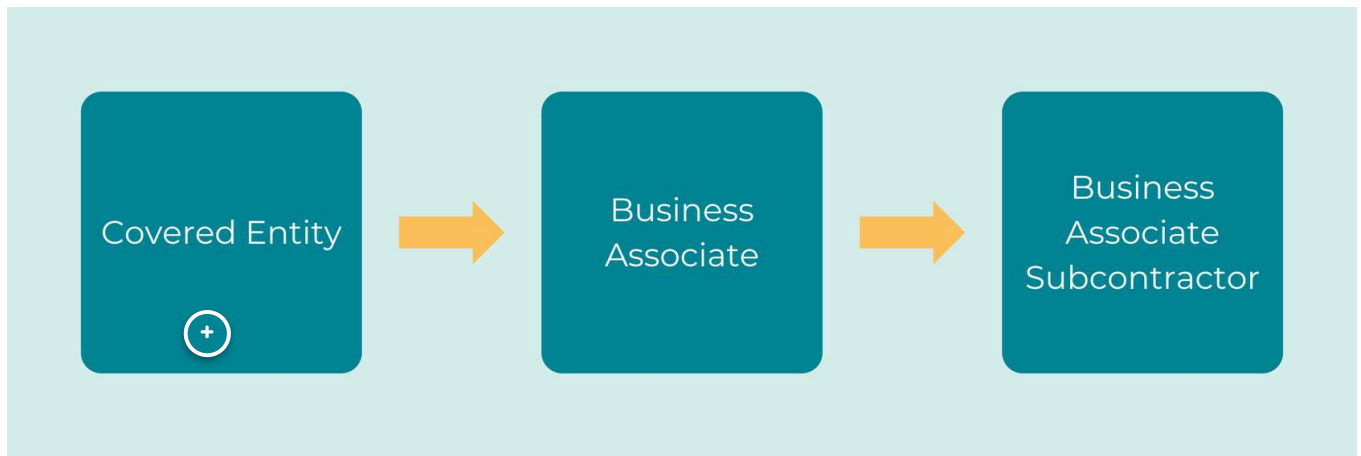
### Not a Conduit

- ✗ Cloud Service Provider
- ✗ Online Backup Service
- ✗ Email Provider
- ✗ Phone System that records calls

## Partnering for Privacy

Click on each "+" below to read the definitions for each term.

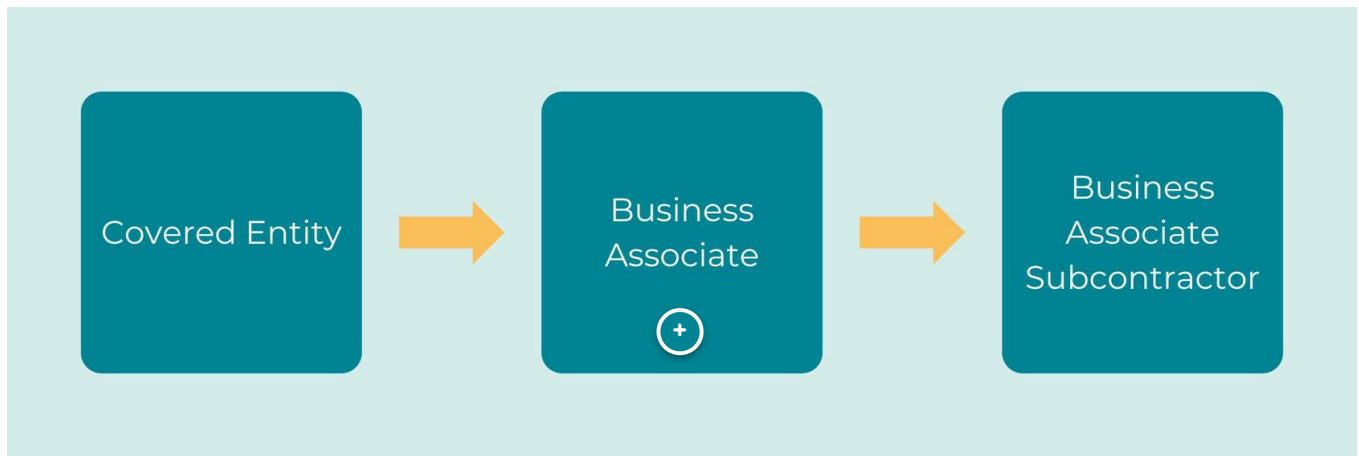




## Covered Entity

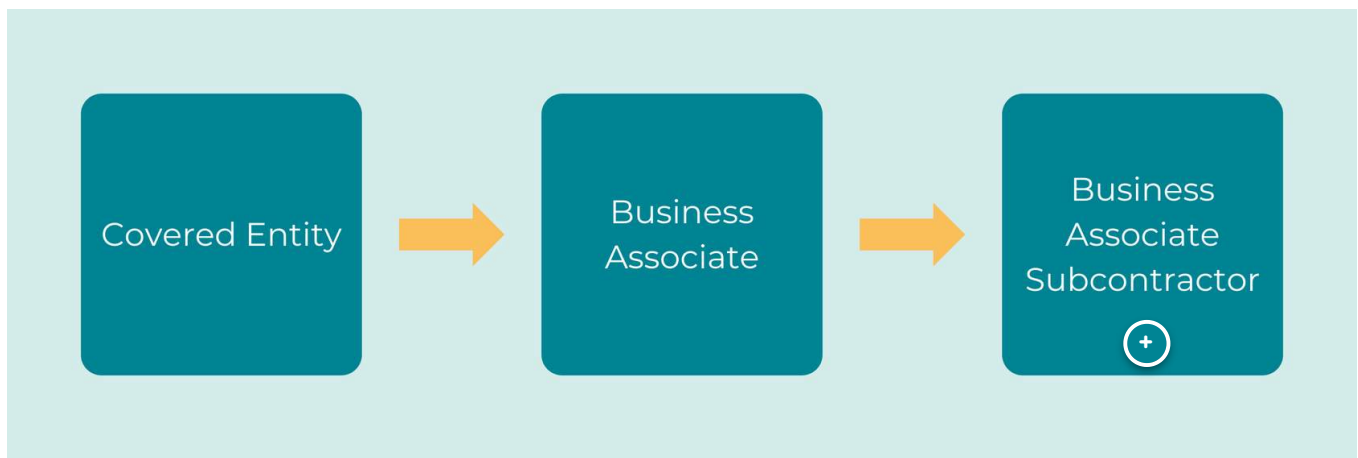
A **covered entity** is a healthcare provider or health plan that provides services to patients.





## **Business Associate**

**Business Associates** are vendors who “create, receive, maintain or transmit” PHI while performing a service involving the PHI on behalf of a Covered Entity.



### **Business Associate Subcontractor**

Sometimes, a business associate might hire another company or person to help them with their work.

**Business Associate Subcontractors** are vendors who “create, receive, maintain or transmit” PHI while performing a service involving the PHI on behalf of a Business Associate.

#### **Here's how it works with Privia:**

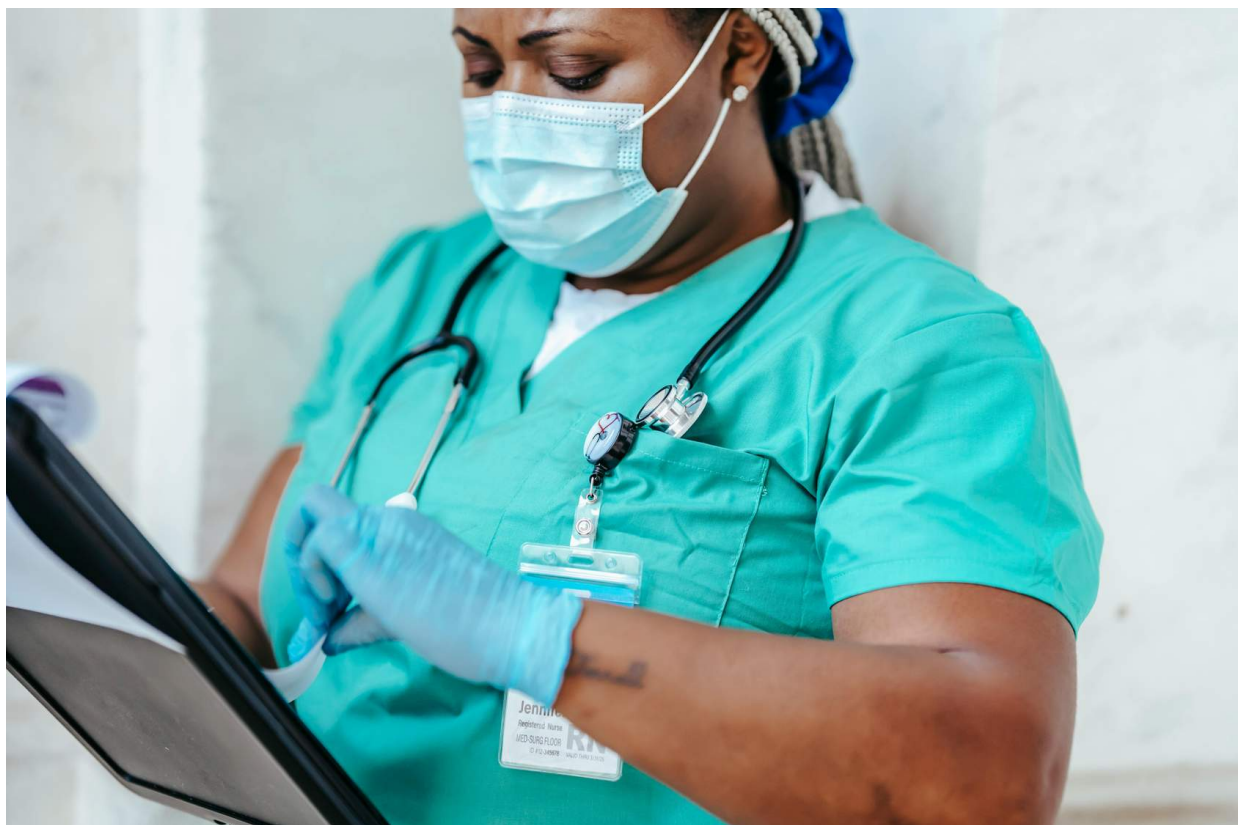
- Privia Medical Group is like the main doctor's office. They are responsible for protecting all patient health information.
- Your Care Center is a business associate to Privia Medical Group. The practice works on behalf of Privia, but you also might hire your own helpers (business associates).
- Your Business Associates are the companies or people YOU hire to help with tasks that involve patient information. These are not Privia's business associates.

**Example:** If your Care Center hires a scribe service (someone who helps doctors with their notes), that scribe service is YOUR business associate, not Privia's. But since they're doing work for

you, and you're working on behalf of Privia, they also become a "business associate subcontractor" to Privia. Privia Medical Group is like the main doctor's office. They are responsible for protecting all patient health information.



Complete the content above before moving on.



### **Your Responsibility:**

It's **YOUR** job to make sure any company or person you hire (your business associates) knows how to protect patient information properly. This means:

- Making sure they have a signed contract that says they'll follow all the rules.

- Checking that they have safeguards in place to prevent unauthorized access, use, disclosure, or alteration of patient health information.
- Making sure they know what to do if there's ever a data breach.

---

## **Why is this important?**

Protecting patient health information is crucial! If this information gets into the wrong hands, it can lead to identity theft, fraud, and other serious problems. By making sure everyone who handles this information does so responsibly, we can keep patients safe.

**CONTINUE**

# Business Associate Agreements (BAAs): The Foundation of Secure Partnerships

Business Associate Agreements (BAAs) are the cornerstone of protecting patient health information (PHI) when working with external vendors or partners. These legally binding contracts establish a framework of trust and shared responsibility between your care center and your business associates, ensuring everyone understands their role in safeguarding sensitive data. By clearly defining permitted uses, requiring robust safeguards, and outlining procedures for breach notification, BAAs help maintain compliance with HIPAA and build a culture of security.

## What is a Business Associate Agreement (BAA)? —

A legal contract required by HIPAA between a Covered Entity (CE) and its Business Associate (BA) to protect Patient Health Information (PHI). BAAs are also required between BAs and their subcontractors.



## Why do BAAs matter? —

Business Associate Agreements (BAAs) are essential legal contracts mandated by HIPAA. They serve as the foundation for protecting patient health information (PHI) by clearly defining the responsibilities and obligations of both covered entities (like Privia Medical Group) and their business associates. BAAs ensure that everyone involved in handling PHI understands their role in safeguarding sensitive data, preventing unauthorized access or disclosure. Furthermore, BAAs are a critical component of preparedness for potential investigations, as they are often the first document requested by the Department of Health and Human Services (HHS) in the event of a data breach.



## Key Elements of a BAA —

- Describes the permitted uses and disclosures of PHI by the BA
- Prohibits other uses or further disclosures of PHI
- Requires appropriate safeguards to prevent impermissible uses or disclosures
- Requires notification of any breach of PHI
- Includes indemnification and insurance provisions to protect the Covered Entity



## Managing Your Business Associates —

Effectively managing your business associates is crucial to safeguarding patient data and ensuring compliance. Follow these essential steps to establish and maintain secure partnerships:

- **Maintain an inventory:** Keep a detailed list of all your business associates
- **Verify insurance:** Obtain proof of cyber-liability insurance (typically exceeding \$5 million) before contracting with a new business associate
- **Onboard workforce members:** Add all business associate staff who need access to Privia systems to your roster, requiring them to sign necessary agreements, including confidentiality agreements (Privia collects signature when creating account)
- **Consider periodic audits:** Regularly assess your business associates' compliance with regulations and agreements to maintain data security





Complete the content above before moving on.



**Business Associate Agreements** are a critical component of protecting patient health information and ensuring HIPAA compliance. By establishing clear responsibilities and safeguards, BAAs create a framework for secure partnerships that prioritize patient privacy. If you have any questions or need further guidance, please don't hesitate to reach out to your Compliance Liaison.

CONTINUE

# Safeguarding Patient Data: Understanding Privia's Third-Party Access Committee (TPAC)

## Third Party Access Review



Protecting patient information is paramount to maintaining trust and upholding the highest standards of care. However, granting third-party vendors access to electronic protected health information (ePHI), while necessary for various services, can introduce significant risks. Unauthorized access, accidental disclosures, or even malicious attacks can lead to data breaches, compromising patient privacy and potentially causing harm. To mitigate these risks,

Privia has implemented a rigorous review process through the Third-Party Access Committee (TPAC).

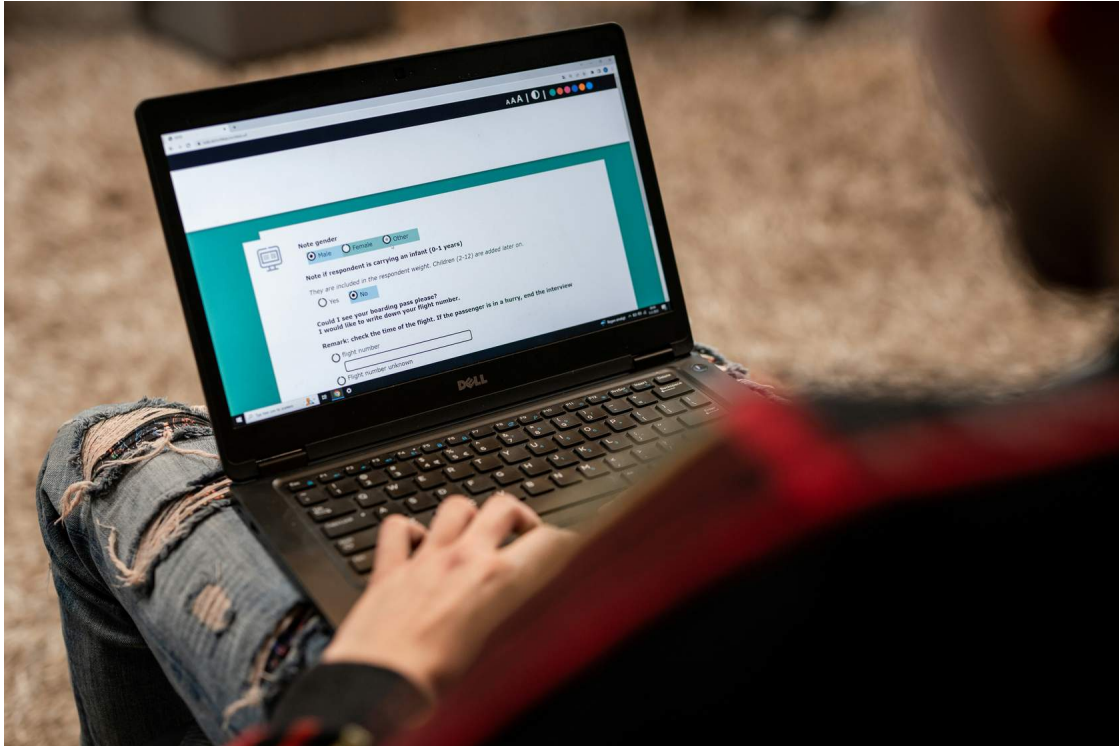
Any of your business associates who need access to ePHI beyond end-user access in athena, such as an interface, data feed, reports, access to the athena API, or will store Privia ePHI, need to be reviewed by Privia's Third-Party Access Committee (TPAC).

**Click 'Start' below to explore the third party access review process.**

## Third Party Access Review Process



## Questionnaire



All third parties that require access to ePHI must complete Privia's questionnaire to ensure the confidentiality of our patient information and ensure compliance with all applicable security regulations and payer requirements.



## Committee Review



TPAC reviews the questionnaire and may request additional information or clarification. One goal of the committee is to balance innovation and flexibility for Care Centers while safeguarding patient information and protecting the Care Center and the Medical Group.

## Access Agreement



Once approved, the third party must sign a Third Party Access Agreement with Privia Health and a Business Associate Agreement with the Care Center.



## How to Submit a Third Party for Review

- Send the potential business associate the [link](#) to the TPAC questionnaire.
- Completed forms are added to the next review agenda.
- For questions or status updates, email [TPAC@priviahealth.com](mailto:TPAC@priviahealth.com).

## What Does TPAC Evaluate?

**Data and Use:** Understand what patient data the vendor will access and how it will be used.

**ePHI Storage and Encryption:** Ensure data is securely stored and encrypted, with a focus on offshore use protocols.

**Technology Specs and Requirements:** Verify compatibility with Privia's systems.

**Risk Reduction:** Assess the overall risk to Privia and patients.

## **Termination of a Third Party Access Agreement / Third Party Incident**

In the event of a cybersecurity incident, Privia reserves all rights to terminate at its discretion access to the Privia Platform and/or athenaOne to ensure the safety and privacy of patient and Care Center Data.

In the event that a third party does not meet Privia's required safeguards on its control verification every other year, Privia will give existing vendors an opportunity to cure the deficiencies. Failure to work on corrective action plans may result in termination of their ability to connect to the Privia Platform and/or athenaOne. Privia will make every attempt to notify impacted Care Centers, however the impacted vendor is responsible for making those notifications.

## Summary

The Third-Party Access Committee (TPAC) is your partner in protecting patient data while utilizing third-party services. Remember, any vendor needing access beyond standard Athena use must undergo TPAC review. Submitting a request is simple: share the TPAC questionnaire link with the vendor. TPAC evaluates data usage, security, compatibility, and risk to ensure patient privacy. Partnering with TPAC upholds our commitment to data security.



Complete the content above before moving on.

### Quick Check

Which of the following scenarios requires review by Privia's Third-Party Access Committee (TPAC)?

---



A business associate will be storing Privia's electronic protected health information (ePHI) on their own servers.



A Care Center staff member needs to access a patient's medical record.

SUBMIT

What is the main purpose of the Third-Party Access Committee (TPAC)?

---

- ☐ To negotiate contracts with third-party vendors.
- ☐ To train Care Center staff on HIPAA compliance.
- ☐ To evaluate and mitigate the risks associated with third-party access to patient data.
- ☐ To provide technical support for using third-party applications.

SUBMIT



Complete the content above before moving on.

# Implementing the HIPAA Security Rule: Your Role as a Privia Business Associate



As a Privia Business Associate, you play a crucial role in safeguarding electronic protected health information (ePHI). Understanding and implementing the HIPAA Security Rule is essential to protecting patient data and ensuring compliance.

## Key Elements of the HIPAA Security Rule

The HIPAA Security Rule requires covered entities and business associates to implement **administrative**, **technical**, and **physical** safeguards to protect ePHI. As a Business Associate, each Care Center is responsible for adopting their own HIPAA

Security policies based on their operations. Policies & Procedures are requested by HHS in all breach investigations.

These safeguards are designed to ensure the confidentiality, integrity, and availability of ePHI.

CONTINUE

## Developing Your Security Policies



### Action: Draft Security Policies

- Review previous Security Risk Assessments for any policy gaps.
- Review [HHS HIPAA Security Series](#) to understand policy requirements.

- Review Privia's HIPAA Security Policies on Privia Connect.
- **Reference:** [HHS Audit Protocol](#)
- Review Privia's HIPAA Security Policy Blueprints on Privia Connect.

## Health and Human Services

HHS developed a HIPAA Security Series that has detailed information about the following:

**Administrative** actions, policies, and procedures, to manage implementation, and maintenance of security measures to protect ePHI

**Physical** measures, policies, and procedures to protect a Covered Entity's information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion

**Technical** includes technology safeguards and the policy and procedures for its use that protect ePHI and control access to it





CONTINUE

# Safeguarding Patient Data: Understanding Your Annual Security Risk Assessment (SRA)

The HIPAA Security Rule and Privia's commitment to value-based care require all Care Centers to conduct an annual Security Risk Assessment (SRA). This process helps identify and address vulnerabilities in your systems and processes that could compromise patient data.

## Why is SRA Important?

### Legal Requirement —

The HIPAA Security Rule and the Merit-based Incentive Payment System (MIPS) value-based care program both mandate annual Security Risk Assessments (SRAs) for all healthcare organizations that handle electronic protected health information (ePHI). Failure to comply with this requirement can result in penalties and jeopardize your participation in value-based care programs.



## Protecting Patient Data —

SRAs are not just a legal requirement; they are a vital tool for proactively identifying and mitigating risks to patient data. By conducting a thorough SRA, you can uncover vulnerabilities in your systems, processes, and policies that could potentially lead to data breaches. Taking corrective action based on your SRA findings helps safeguard sensitive patient information and maintain the trust of those you serve.



## Compliance Attestation —

The results of your annual SRA are a critical component of Privia Medical Group's compliance attestation to the Centers for Medicare & Medicaid Services (CMS) and other value-based care payers. This attestation verifies that Privia and its affiliated Care Centers are adhering to the security requirements necessary to protect patient information and ensure the integrity of healthcare programs.



Complete the content above before moving on.

## Completing Your Annual SRA

Click 'START' below to view the process for completing your SRA.

## **Completing Your Annual Security Risk Assessment (SRA)**

## Engage a Third-Party Expert (Recommended)



Privia strongly recommends contracting with a third-party security expert to conduct your SRA. This ensures a thorough, objective assessment that meets industry standards and is well-prepared for potential audits.

Privia maintains a list of qualified providers offering discounted services to our Care Centers.

**Tip:** Engaging an expert can save time and resources while ensuring a high-quality assessment.



## Analyze Risks



With your chosen expert (or internally, if you choose), thoroughly assess all potential risks to patient information, considering both internal and external threats.

Evaluate the likelihood and potential impact of each risk.

**Tip:** Every year Privia releases a Statement of Security standards based on the results of Privia's Enterprise Security Risk Assessment that summarizes the security controls Privia administers on behalf of Care Centers. Utilize [Privia's Statement of Security Standards](#) to understand the controls Privia has in place.

## Identify Gaps

Compare your current security measures to the identified risks.

Determine areas where your safeguards are insufficient or where additional protections are needed.

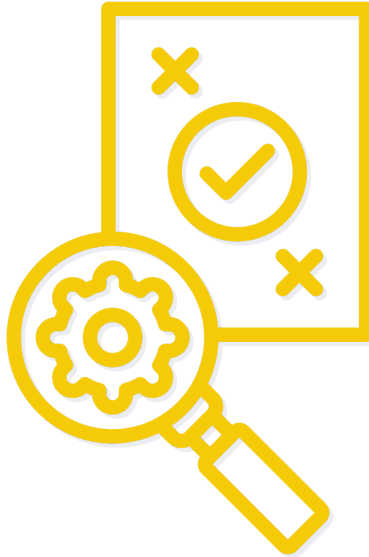
**Tip:** The [HHS Security Risk Tool](#) provides valuable guidance and sample questions to help you identify potential gaps. (Windows Only)

### Other Resources:

[SRA Tool Training Presentation](#)

[SRA Tool User Guide](#)

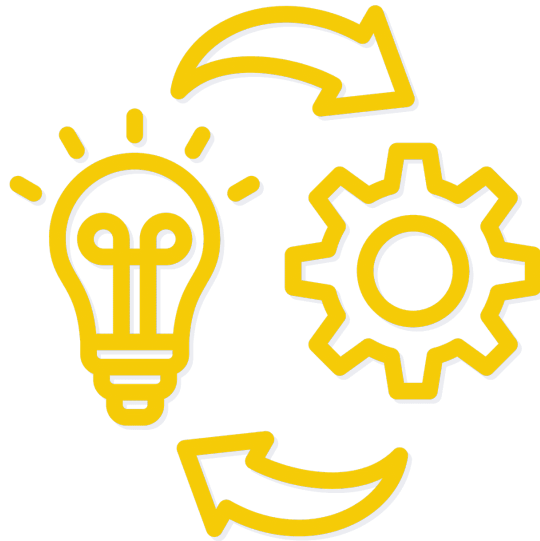
## Develop a Corrective Action Plan



Create a detailed plan to address the identified gaps and mitigate the associated risks.

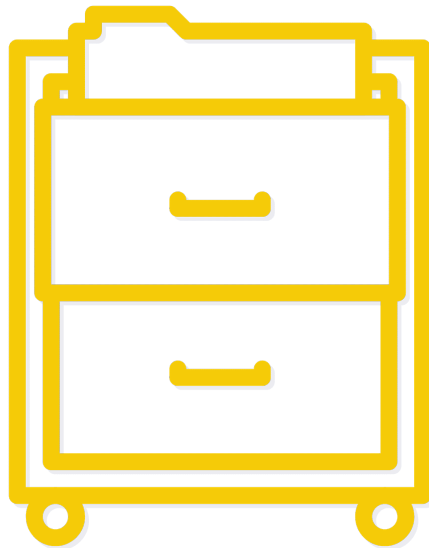
Prioritize actions based on the level of risk and potential impact.

## Implement and Monitor



- Put your corrective action plan into action.
- Regularly monitor the effectiveness of your implemented measures.
- Adjust your plan as needed based on ongoing risk assessments.

## Retain Records



- Keep records of all completed SRAs for at least six years.
- This documentation is essential for demonstrating compliance and tracking your progress over time.

## Summary

Annual security risk assessments (SRAs) are a critical requirement for protecting patient data and ensuring compliance. SRAs help identify vulnerabilities and mitigate risks to prevent data breaches. Privia strongly recommends engaging a third-party expert for a thorough assessment, and provides resources to guide you through the process. Remember, regular SRAs are essential for safeguarding patient privacy and maintaining the integrity of your healthcare operations.



Complete the content above before moving on.



### **Steps to Complete Security Risk Assessment**

- Download [Privia Statement of Security Standards](#)
- Review [HHS Guidance on conducting risk analysis](#).
- Conduct Security Risk Assessment using [HHS SRA Tool](#) or Third Party Vendor (Privia highly recommends using a third-party to complete your Risk Assessment)

- Complete Information Security Survey & SRA Attestation

## Privia's Annual Attestation: Your Role in Demonstrating Compliance

In addition to conducting your Security Risk Assessment (SRA), all Privia care centers must complete an annual attestation to confirm their compliance with security, privacy, and other regulatory requirements.

- **Purpose:** This attestation provides assurance to Privia Medical Group, CMS, and other value-based care payers that your care center is actively maintaining a secure environment for patient data, and is required in order for Privia and Care Centers to continue to qualify for several value based payment agreements including MIPS
- **Timing:** The attestation survey is typically sent out in mid-July and should be completed by the end of September.
- **Recipients:** Office managers, compliance liaisons, and physician owners will receive the survey.
- **Distinct from SRA:** Remember, this attestation is separate from your annual SRA. While both are important for compliance, the SRA focuses on identifying and addressing risks, while the attestation confirms adherence to a broader set of requirements.
- **Survey results:** Results are shared with the Privia Medical Group Board & Compliance Committee in each market.

CONTINUE

---

By conducting a comprehensive annual SRA, you proactively protect patient data, maintain compliance, and contribute to the overall security of Privia's healthcare ecosystem. If you have any questions,



please consult your Compliance Liaison or refer to the resources available on Privia Connect.

**CONTINUE**

# Workforce Authorization

## Maintaining a Secure Workforce Roster: Your Role in Data Protection



### Why a Secure Roster Matters

The workforce roster serves as the gatekeeper to Privia's systems and the sensitive patient health information (PHI) they contain. Maintaining an accurate and up-to-date roster is essential to ensuring that only authorized individuals have the appropriate access to this data.

Unauthorized access, whether intentional or accidental, can lead to serious consequences, including data breaches, privacy violations, and potential harm to patients. By understanding your role in managing the roster, you contribute to the protection of patient privacy and the overall security of Privia's health information systems.

## Key Roles and Responsibilities

Select the (+) on the tabs below to read more.

### Compliance Liaison and Privia Connect Admins —

The Compliance Liaison and Privia Connect Admins play vital and complementary roles in maintaining the accuracy and security of the workforce roster:

#### Compliance Liaison:

- Oversees the roster at the Care Center level.
- Ensures that the roster accurately reflects the current workforce and their access needs.
- Collaborates with Privia Connect Admins to address any discrepancies or issues.
- Promotes awareness of roster security among care center staff.

#### Privia Connect Admins:

- Have been delegated the authority to update the workforce roster on Privia Connect.
- Work in partnership with Compliance Liaisons to ensure timely updates and accuracy.
- Are authorized by the affiliated covered entity to make necessary changes to the roster.

Both roles share the ultimate responsibility of ensuring the roster is up-to-date, reflects the minimum necessary access for each individual, and aligns with Privia's security policies and HIPAA regulations. This collaboration is key to maintaining a secure and compliant environment for patient health information.

### Authorized Representative —

As an Authorized Representative, your responsibilities are crucial for maintaining data security and compliance:

- **Roster Management:** You are responsible for adding new team members, updating existing information, and promptly removing those who no longer require access within 24 hours of any status change.
- **Minimum Necessary Access:** You must ensure that each individual on the roster has the minimum level of access needed to perform their job functions, adhering to the principle of "least privilege."
- **Policy Adherence:** You are expected to understand and follow Privia's HIPAA [Workforce Security and Information Access Management](#), ensuring that all roster activity aligns with these guidelines.

By fulfilling these responsibilities, you play a vital role in protecting sensitive patient data and upholding the integrity of Privia's information systems.



Complete the content above before moving on.

## Managing the Workforce Roster

Select the tabs along the top to read more.

MANAGING THE WORKFORCE  
ROSTER

ROSTER HOW-TO GUIDES

KEY POINTS FOR MANAGING  
WORKFORCE ROSTER ACCESS

## Managing the Workforce Roster



**MANAGING THE WORKFORCE  
ROSTER**

**ROSTER HOW-TO GUIDES**

**KEY POINTS FOR MANAGING  
WORKFORCE ROSTER ACCESS**

## **Resources:**

[Adding a New Team Member](#)

[Roster Verification and Workflow](#)

These resources are on Privia Connect and will require your Privia Connect login to view.

# Roster How To



MANAGING THE WORKFORCE  
ROSTER

ROSTER HOW-TO GUIDES

KEY POINTS FOR MANAGING  
WORKFORCE ROSTER  
ACCESS

- **Accuracy is Key:** Ensure all team member information is entered correctly, including their roles and permissions, to prevent unauthorized access to sensitive patient data.
- **Least Privilege Principle:** Grant each team member only the minimum level of access necessary to perform their job duties. This helps minimize the risk of accidental or intentional data breaches.
- **Prompt Action:** When a team member's employment status or role changes, promptly update the roster within 24 hours to ensure that their access to Privia systems reflects their current responsibilities.

- **Regular Review:** Periodically review the roster to confirm its accuracy and verify that all team members still require access to the systems and data they are assigned. This practice helps maintain a secure and compliant environment for patient health information.



Complete the content above before moving on.

Maintaining an accurate workforce roster, in collaboration with Compliance Liaisons, is crucial for protecting patient information. This adherence to the principle of least privilege helps safeguard patient data and ensures compliance.

CONTINUE

## Safeguarding Your Center

### HIPAA Enforcement Rule





The HIPAA Enforcement Rule outlines penalties for non-compliance, emphasizing the importance of safeguarding patient data.

In this section we'll delve into the consequences of HIPAA violations, the crucial role of cyber liability insurance, and the essential technical controls that protect your Care Center from cyber attacks.


| HHS ENFORCEMENT AUTHORITY   | COMMON HIPAA VIOLATIONS RESULTING IN FINES FOR BUSINESS ASSOCIATES | BREACH STATISTICS | TIERED PENALTY STRUCTURE |
|---|--|-------------------|--------------------------|
| <p>The Department of Health and Human Services (HHS) has the authority to impose fines for violations of the Health Insurance Portability and Accountability Act (HIPAA). These enforcement actions often focus on breaches impacting 500 or more patients, but smaller breaches can also be subject to penalties. Fines are calculated on a per-record basis, meaning each individual whose information was compromised can result in a separate fine, with a maximum annual limit. Key Enforcement Provisions:</p> <ul style="list-style-type: none"><li>• <b>Affiliated Covered Entities:</b> If a covered entity is part of a larger affiliated group, each member can be held jointly and severally liable for HIPAA violations unless it can be proven that a specific member was solely responsible.</li><li>• <b>Liability for Agents:</b> Covered entities (like Privia Medical Group) are liable for the actions of their workforce members and business associates. Similarly, business associates are liable for the actions of their workforce members and subcontractors. This means everyone in the chain of responsibility is accountable for maintaining HIPAA compliance.</li></ul> |  |                   |                          |

| HHS ENFORCEMENT AUTHORITY  | COMMON HIPAA VIOLATIONS RESULTING IN FINES FOR BUSINESS ASSOCIATES | BREACH STATISTICS | TIERED PENALTY STRUCTURE |
|--|--|-------------------|--------------------------|
| <p>Business associates, like healthcare providers, are subject to HIPAA regulations and can face significant fines for non-compliance. Here are some common violations that have led to penalties for business associates:</p> <ul style="list-style-type: none"><li>• <b>Failure to Conduct a Security Risk Assessment (SRA):</b> Neglecting to perform a comprehensive SRA to identify and address potential vulnerabilities in your systems and</li></ul> |  |                   |                          |

processes.

- **Failure to Remediate Identified Risks:** Not taking corrective action to address vulnerabilities identified during an SRA or through other means.
- **Lack of Business Associate Agreements (BAAs):** Failing to have a signed BAA with subcontractors who handle PHI on your behalf.
- **Impermissible Uses and Disclosures of PHI:** Using or disclosing PHI in a way that is not permitted by HIPAA or your BAA with the covered entity.
- **Failure to Provide Breach Notification:** Not promptly notifying the covered entity or affected individuals of a breach of unsecured PHI.
- **Failure to Implement Safeguards:** Not having appropriate administrative, technical, and physical safeguards in place to protect ePHI.
- **Failure to Cooperate with HHS Investigations:** Not responding to requests for information or cooperating with HHS investigations into potential HIPAA violations.

| HHS ENFORCEMENT<br>AUTHORITY   | COMMON HIPAA<br>VIOLATIONS<br>RESULTING IN FINES<br>FOR BUSINESS<br>ASSOCIATES | BREACH STATISTICS | TIERED PENALTY<br>STRUCTURE |
|--|--|-------------------|-----------------------------|
| <ul style="list-style-type: none"><li>• The average cost of a healthcare data breach is <b>\$10.93</b> million dollars.</li><li>• The healthcare industry has the highest cost associated with a data breach for the <b>13th year</b> in a row.</li><li>• <b>1/3</b> of all breaches are identified by an organization's own security teams/tools.</li><li>• There has been a <b>53%</b> increase in the cost of a healthcare data breach since 2020.</li><li>• <b>82%</b> of the data involved in breaches is stored in the cloud.</li><li>• The average time it takes to recover from a breach is <b>277</b> days, 204 days on average to identify the breach and another 73 days to contain the breach.</li><li>• <b>68%</b> of breaches involve a non-malicious human element.</li></ul> |  |                   |                             |

| HHS ENFORCEMENT<br>AUTHORITY  | COMMON HIPAA<br>VIOLATIONS<br>RESULTING IN FINES<br>FOR BUSINESS<br>ASSOCIATES  | BREACH STATISTICS  | TIERED PENALTY<br>STRUCTURE |               |   |  |               |   |  |               |  |   |               |   |  |   |  |  |
|---|---|--|-----------------------------|---------------|---|--|---------------|---|--|---------------|--|---|---------------|---|--|---|--|--|
| <div><div>Health &amp; Human Services<br/>HIPAA Enforcement   2025 Fines</div><table><tr><td><b>Tier 1</b></td><td><b>No Knowledge</b><br/>Did not know and could not reasonably have known of the breach</td><td><b>\$141 - \$71,162</b><br/><i>per violation / record</i></td></tr><tr><td><b>Tier 2</b></td><td><b>Reasonable Cause</b><br/>“Knew” or by exercising reasonable diligence, “would have known” of the violation, did not act with willful neglect.</td><td><b>\$1,424 - \$71,162</b><br/><i>per violation / record</i></td></tr><tr><td><b>Tier 3</b></td><td><b>Willful Neglect   Corrective Action Taken</b><br/>“Acted with willful neglect” and corrected the problem within a 30-day time period</td><td><b>\$14,232 - \$71,162</b><br/><i>per violation / record</i></td></tr><tr><td><b>Tier 4</b></td><td><b>Willful Neglect   No Action Taken</b><br/>“Acted with willful neglect” and failed to make a timely correction</td><td><b>\$71,162 - \$2,134,831</b><br/><i>per violation / record</i></td></tr><tr><td colspan="2"><small>Source:<br/>Federal Register Annual Civil Monetary Penalties Inflation Adjustment - March 17, 2022</small></td><td><b>\$2,134,831</b><br/><i>Calendar Year Maximum for all Tiers</i></td></tr></table></div> |   |  |                             | <b>Tier 1</b> | <b>No Knowledge</b><br>Did not know and could not reasonably have known of the breach | <b>\$141 - \$71,162</b><br><i>per violation / record</i> | <b>Tier 2</b> | <b>Reasonable Cause</b><br>“Knew” or by exercising reasonable diligence, “would have known” of the violation, did not act with willful neglect. | <b>\$1,424 - \$71,162</b><br><i>per violation / record</i> | <b>Tier 3</b> | <b>Willful Neglect   Corrective Action Taken</b><br>“Acted with willful neglect” and corrected the problem within a 30-day time period | <b>\$14,232 - \$71,162</b><br><i>per violation / record</i> | <b>Tier 4</b> | <b>Willful Neglect   No Action Taken</b><br>“Acted with willful neglect” and failed to make a timely correction | <b>\$71,162 - \$2,134,831</b><br><i>per violation / record</i> | <small>Source:<br/>Federal Register Annual Civil Monetary Penalties Inflation Adjustment - March 17, 2022</small> |  | <b>\$2,134,831</b><br><i>Calendar Year Maximum for all Tiers</i> |
| <b>Tier 1</b>   | <b>No Knowledge</b><br>Did not know and could not reasonably have known of the breach   | <b>\$141 - \$71,162</b><br><i>per violation / record</i>         |                             |               |   |  |               |   |  |               |  |   |               |   |  |   |  |  |
| <b>Tier 2</b>   | <b>Reasonable Cause</b><br>“Knew” or by exercising reasonable diligence, “would have known” of the violation, did not act with willful neglect. | <b>\$1,424 - \$71,162</b><br><i>per violation / record</i>       |                             |               |   |  |               |   |  |               |  |   |               |   |  |   |  |  |
| <b>Tier 3</b>   | <b>Willful Neglect   Corrective Action Taken</b><br>“Acted with willful neglect” and corrected the problem within a 30-day time period          | <b>\$14,232 - \$71,162</b><br><i>per violation / record</i>      |                             |               |   |  |               |   |  |               |  |   |               |   |  |   |  |  |
| <b>Tier 4</b>   | <b>Willful Neglect   No Action Taken</b><br>“Acted with willful neglect” and failed to make a timely correction                                 | <b>\$71,162 - \$2,134,831</b><br><i>per violation / record</i>   |                             |               |   |  |               |   |  |               |  |   |               |   |  |   |  |  |
| <small>Source:<br/>Federal Register Annual Civil Monetary Penalties Inflation Adjustment - March 17, 2022</small>   |   | <b>\$2,134,831</b><br><i>Calendar Year Maximum for all Tiers</i> |                             |               |   |  |               |   |  |               |  |   |               |   |  |   |  |  |



Complete the content above before moving on.

## The Importance of Cyber Liability Insurance: Protecting Your Care Center

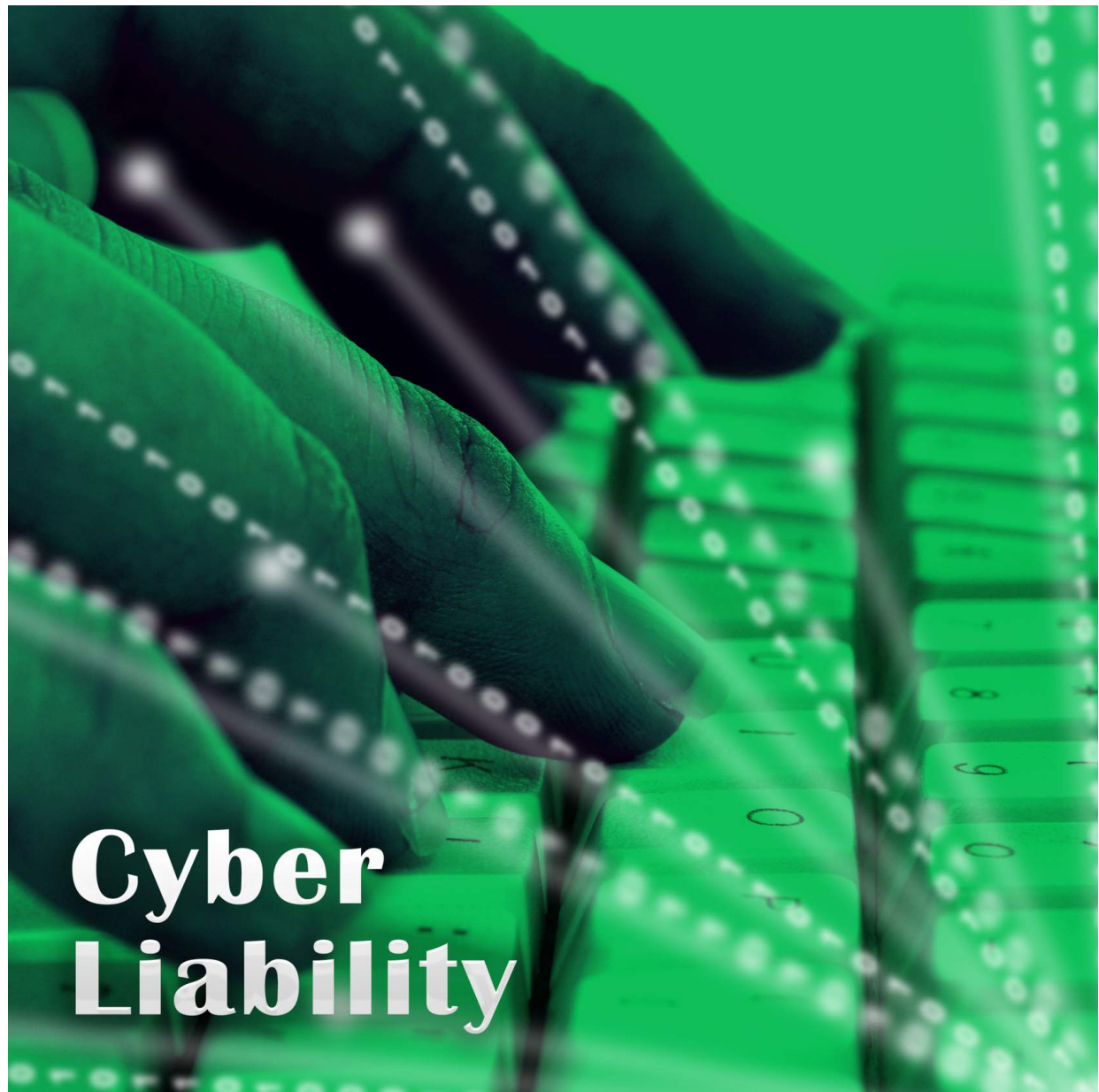
Cyberattacks are a growing threat to healthcare organizations, often resulting in significant financial losses and damage to reputation. Cyber liability insurance is crucial for mitigating these risks.

### Key Points:

- **High Costs:** Investigations and breach remediation are expensive, even without a confirmed breach.
- **Malware Risk:** Malware is considered a reportable breach, further increasing costs.
- **Essential Coverage:** Cyber liability insurance helps cover investigation costs, breach notification, legal fees, fines, and reputational damage.
- **Recommended Coverage:** Privia suggests at least \$1 million for cyber liability and \$3 million for overall data security.
- **Tailored Coverage:** Consult an insurance broker to assess your specific needs, as coverage requirements vary based on factors like patient volume and services offered.
- **Privia Requirements:** Adequate cyber liability coverage is mandatory under your BAA with Privia, and you must confirm your policy details during the annual attestation.



**Remember: Malpractice insurance typically does not cover cyberattacks.**



### **Cyber Liability Insurance Responsibilities:**

- Contact your insurance broker for personalized guidance and assess appropriate coverage amounts.
- Secure a policy.
- Attest in your annual Security Risk Assessment Attestation you have coverage.

- Review [Privia's Cyber Liability Insurance Guidance Document](#) on Privia Connect for more information.

**For questions email:**

[security@priviahealth.com](mailto:security@priviahealth.com)

CONTINUE

## Technical Controls & Managed Security Services: Protecting Your Care Center's Digital Frontline



The most important part of your cyber security program is implementing **technical controls** to prevent threat actors from gaining unauthorized access to your systems and compromising patient data. **Technical controls** are the digital safeguards that protect your Care Center's

systems and data from cyber threats. This section will explore the critical controls required by HIPAA, and how Privia's managed services can help you implement and maintain them.



HHS evaluates the presence of a control and alignment with best practices in the event of a breach investigation in accordance with their [Audit Protocol](#).

CONTINUE

## Examples of 405(d) Cybersecurity Practices

[405\(d\)](#) is a collaborative effort between the government and the healthcare industry to develop cybersecurity standards and best practices that protect patient safety. Below you will find examples of technical controls, this is not a comprehensive list of required technical controls but highlights of key controls required by Care Centers and are included in Privia's Managed Security Services. Click on each (+) below to learn more.

### Email Protection —

To ensure the security and privacy of your email communications, it's crucial to have the following measures in place:

- **Business Class Email:** Choose a professional email provider specifically designed for businesses, not consumer-oriented services like Gmail, Yahoo, or AOL.
- **Signed Business Associate Agreement (BAA):** Make sure you have a BAA in place with your email provider. This legally binding contract ensures they understand and comply with HIPAA regulations regarding your patient data.



- **Encryption:** Your emails should always be encrypted, both when they're being sent ("in transit") and when they're stored ("at rest"). This protects sensitive information from unauthorized access.
- **Technical Standards:** Your email system should support modern security protocols like TLS 2.0, S/MIME, and DLP (Data Loss Prevention) to further safeguard your communications.
- **US-Based Storage:** Choose an email provider that stores your data exclusively within the United States to comply with data privacy regulations and ensure better control over your information.



## Endpoint Protection (Protecting Your Computers) —

**What is an endpoint?** It's simply any device that connects to your network, like your laptops, desktops, or tablets.

- **Supported Operating System (OS):** Using a current, supported operating system ensures your computers receive regular security updates from the manufacturer to protect against vulnerabilities.
- **Monthly Security Updates:** Your computers should receive important security patches every month to fix any weaknesses that hackers could exploit.
- **Optimized for Performance:** Make sure your computers have the necessary processing power and memory to run Privia and athenaOne efficiently.

- **Whole Disk Encryption:** All data on your computers should be encrypted to prevent unauthorized access if the device is lost or stolen.
- **Endpoint Protection Software:** Install comprehensive endpoint protection software that actively safeguards against viruses, malware, and ransomware attacks.

## Data Protection (Servers and Applications) —

If your care center has servers or software that aren't part of Privia's platform, it's crucial to protect them too, as they often contain sensitive patient data. Here's what you need to ensure:

- **Partner with a Local IT Expert:** Servers are prime targets for hackers, so we strongly recommend working with a local IT professional to ensure your systems are configured and maintained securely.
- **Up-to-date Operating System:** Use a supported operating system for your servers that receives regular security updates from the manufacturer.
- **Monthly Security Patches:** Ensure your servers receive and apply all necessary security patches on a monthly basis to address any vulnerabilities.
- **Limited Administrative Access:** Restrict access to your servers by only allowing authorized personnel, and use strong, unique passwords for each user.
- **Whole Disk Encryption:** Encrypt all of your server's data so that even if someone physically accesses the server, the data remains unreadable without the correct decryption keys.
- **Included in Security Risk Analysis (SRA):** Your local IT provider should include your servers and applications in regular security risk assessments to identify and address any potential weaknesses.

While Privia doesn't directly support these systems, we're here to help you understand the best practices for keeping your patient data safe.

## Network Management & Firewalls —

A firewall acts as a shield for your network, controlling what comes in and out. Here's what your firewall needs to keep your network safe:

- **Supported Hardware/Software:** A reliable, up-to-date firewall device that is actively supported by its manufacturer.

- **Quarterly Firmware Updates:** Regular updates to the firewall's internal software (firmware) to ensure it's equipped to handle the latest threats.
- **Detailed Logs:** Maintain detailed logs of all firewall activity for at least 90 days. These logs are essential for investigating potential security breaches.
- **Static IP Address:** A fixed IP address for your firewall to make it easier to manage and monitor.
- **Strict Inbound Traffic Rules:** Block all incoming traffic by default and only allow specific, necessary connections to prevent unauthorized access.
- **Blocked Protocols:** Block specific protocols known to be exploited by hackers, such as NetBIOS (139), RDP (3389), and inbound mail (SMTP).

**Advanced Security (Recommended):**

- **Intrusion Detection & Prevention (IDS/IPS):** We strongly recommend adding this technology to your firewall. It acts like an alarm system, actively monitoring for suspicious activity and stopping attacks in their tracks.



Complete the content above before moving on.

## Privia's Security Guidance Documents (Policy Stat)

Our guidance documents are to assist Care Centers in understanding the minimum required security controls, including compliance with the HIPAA Security Rule, HHS 405(d) cybersecurity practices, applicable local, state, federal laws, and contractual obligations to our private and public payers.



## Security Standards & Controls Guidance

[Security Standards & Controls Toolkit](#)

### Available Guidance Documents

- [Workstation & Endpoint Protection Standards & Controls](#)
- [Firewall Standards & Controls](#)
- [Email & Collaboration Standards & Controls](#)
- [Server & Applications Standards & Controls](#)

### For Questions Email

[security@priviahealth.com](mailto:security@priviahealth.com)

CONTINUE

## Privia's Managed Security Services



### Simplify Your Security with Privia's Managed Services

Privia offers comprehensive managed security services to safeguard your healthcare organization's IT infrastructure. Our services are designed to align with industry-leading cybersecurity practices, including 405(d) recommendations, and can be tailored to protect both newly purchased and existing hardware and software. By partnering with Privia, you can reduce the burden on your Care Center and focus on delivering quality care while ensuring your systems and data remain secure.

#### Here's What We Offer

1

**Supported Workstation:** Included with all Privia workstations, this service ensures your computers are always up-to-date and

secure. We handle patch management, encryption, security configurations, and updates for both Privia and athenaOne software.

2

**Endpoint Protection:** Also included with all Privia workstations, we use Sophos Intercept-X, a market-leading endpoint protection solution. This advanced software is constantly monitored and configured by Privia experts to guard against viruses, malware, and ransomware attacks.

3

**Managed Firewall:** This service, included with all Privia firewalls, provides a robust first line of defense for your network. Our team handles best practices configuration, quarterly security updates, log management, initial security incident response, ongoing monitoring, and VPN management.

4

**Google Workspace Enterprise:** Our managed Google Workspace solution gives you a secure, HIPAA-compliant platform for email and collaboration. Our healthcare technology experts ensure your communication tools are protected and optimized for your needs.

5

**Value Added Managed Security Services:** Any hardware or software purchased from Privia includes our value-added managed security services for the supported lifetime of the device or service. We also offer a one-time setup fee for existing workstations that meet our minimum requirements. Devices are eligible for Privia support as long as they continue to meet or exceed athenaHealth's technical requirements and are still supported by the manufacturer, operating system vendor, meet minimum security requirements, and have Privia's endpoint management software installed.

By partnering with Privia for your cybersecurity needs, you're choosing a dedicated team of experts who understand the unique challenges faced by healthcare organizations. We take care of the technical details so you can focus on what matters most – your patients.

**SIMPLY YOUR SECURITY**

**SUPPORTED TIER**

**MANAGED TIER**

Privia's Managed Security helps to reduce your information security burden. Click each tab to read about the support tiers offered by Privia.



**SIMPLY YOUR SECURITY**

**SUPPORTED TIER**

**MANAGED TIER**

**Privia Supported Tier: Comprehensive Security and Support for Your Practice**

Ideal for large care centers with a moderate security burden, our Supported Tier combines robust cybersecurity protection with expert remote support services.

**Cybersecurity Protection:**

- **Managed Workstation & Endpoint Protection:** Privia handles all standard security measures for your workstations, ensuring compliance with HIPAA and industry best practices. We provide continuous monitoring and protection against viruses, malware, and ransomware, so you can focus on patient care.

**Remote Support Services:**

- **Service Desk (24/7):** Our experienced support team is available during business hours to help you with any technical issues or questions.
- **Operating System & Application Support:** Get assistance with basic operating system issues, Privia and athenaOne applications, and Chrome browser.
- **Hardware Support:** We provide support for Ingenico credit card machines (Elavon), basic IP printing and label printers, ID card scanners, and Midmark & Welch Allyn PFT, EKG, ECG devices.
- **Next-Day Credit Card Machine Replacement:** We understand the importance of keeping your practice running smoothly, so we offer next-day replacement for your credit card machines.

**Included with Purchase or One-Time Setup Fee:**

This comprehensive support package is included with the purchase of any computer from Privia, or is available for a one-time setup fee on devices that meet our minimum specifications.

| SIMPLY YOUR SECURITY   | SUPPORTED TIER | MANAGED TIER |
|--|----------------|--------------|
| <p><b>Privia Managed Tier:</b> Simplified Security for Small to Mid-Size Care Centers</p> <p>Tailored for small to mid-size care centers with a lower security burden, our Managed Tier focuses on essential firewall protection and proactive security management.</p> <p><b>Cybersecurity Protection:</b></p> <ul style="list-style-type: none"><li>• <b>Managed Firewall:</b> Privia takes full responsibility for your firewall, ensuring it's configured correctly, updated regularly, and monitored for potential threats. This includes managing VPNs (Virtual Private Networks) and responding promptly to any security incidents.</li></ul> |                |              |



### Additional Support Services:

- **ISP Coordination:** We'll work directly with your internet service provider (ISP) to resolve any downtime issues quickly, minimizing disruptions to your practice.
- **On-Site Warranty Replacement:** In the unlikely event of a hardware failure, we'll send a technician to your location to replace your firewall under warranty, ensuring minimal downtime.
- **Daily Firewall Monitoring & Early Response:** Our team continuously monitors your firewall for any signs of trouble, allowing us to proactively address potential security threats.

### Included with Firewall Purchase:

This comprehensive firewall management package is included with the purchase of a firewall from Privia.



Complete the content above before moving on.

## Secure Your Communications with Privia's Managed Google Workspace



**Benefits:**

- **Enhanced security:** Unlike free email, our solution includes encryption, data loss prevention, and robust access controls.
- **HIPAA compliance:** We ensure your email aligns with all HIPAA requirements.
- **Expert management:** Our cybersecurity team handles the technical details so you can focus on patient care.

- **Complete protection:** Our managed Google Workspace includes all the controls outlined in our [Email/Collaboration Security Guidance document](#).



All Care Center workforce members who have access to Privia ePHI are required to have an email that meets the requirements outlined in the [secure email guidance](#).

---

Understanding the HIPAA Enforcement Rule, securing cyber liability insurance, and implementing robust technical controls create a strong defense against cyber threats. With the right resources and partners like Privia, you can confidently navigate the evolving cybersecurity landscape and focus on delivering quality care.

CONTINUE

# Compliance, Privacy, and Security a Year-Round Roadmap



Staying compliant with privacy and security regulations is a year-round effort. This section will guide you through Privia's annual compliance, privacy, and security calendar, highlighting key deadlines and essential resources to help you protect patient data and maintain the integrity of your operations.

## The Year-Round Timeline

### *Quarter 1 & Quarter 2*

#### **Focus on Remediation and Review**

- Address any deficiencies identified in the previous year's Security Risk Assessment (SRA).
- Implement updated security controls based on the latest guidance documents.
- Privia conducts its enterprise-wide security risk assessment.
- April Spring Privacy/Security Update to all Compliance Committee Chairs.

### *May/June: Roster Verification*

#### **Prepare for Annual Compliance Training**

- Care Center rosters must be verified by the beginning of June to prepare for annual compliance training.

### *Quarter 3 (July-September)*

#### **Annual Compliance Activities: Training and Attestation**

- Annual Compliance Training: All workforce members must complete compliance training by the beginning of September.
- Care Center SRA Attestation: Ensure all security controls from the guidance documents have been implemented and complete the attestation form by the end of September.

#### *Early Quarter 4*

#### **Compliance Committee Reporting**

- Fall Privacy/Security report on the completion status of compliance training and security attestation to the Compliance Committee.
- Care Centers with deficiencies will receive follow-up and support to address them.

CONTINUE

---

Follow the compliance calendar and use the available resources to **protect patient data, stay compliant**, and

**avoid fines.** This builds trust with patients and ensures your practice's success.

CONTINUE

# Your Privacy & Security Checklist: A Roadmap to Compliance



Building and maintaining a strong privacy and security program is essential for protecting patient information, avoiding penalties, and maintaining trust. These checklists will guide you through the key elements of an effective program and ensure your care center is in compliance with HIPAA regulations.

## Privacy Checklist

- Maintain a dedicated cyber liability insurance policy.

## Security Checklist

- Perform an annual security risk assessment and attestation.
- Designate an individual responsible for information security.



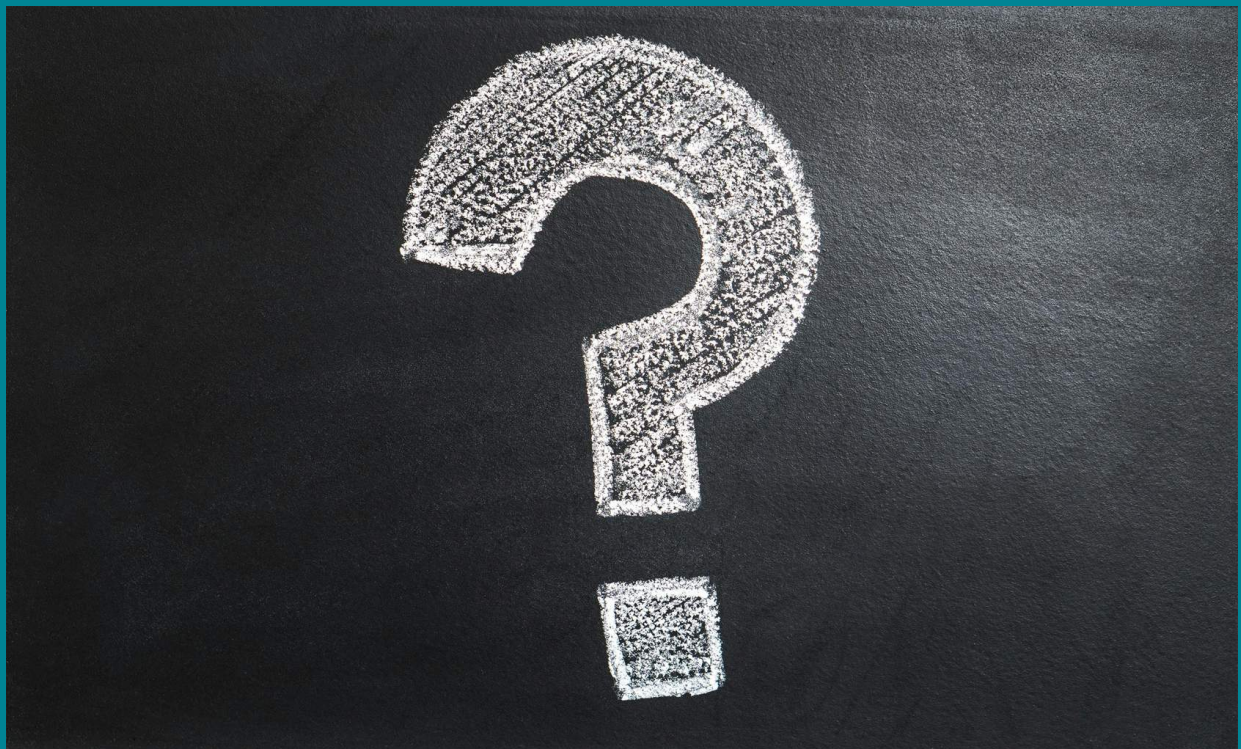
- Ensure all downstream business associates have signed Business Associate Agreements (BAAs).
- Develop care center-specific HIPAA Privacy & Security Policies.
- Submit new business associates who require access to Privia systems for review.
- Complete workforce training annually.
- Report incidents or suspected breaches to [compliance.priviahealth.com](https://compliance.priviahealth.com) ASAP.
- Manage the practice roster periodically.
- Remove workforce members who no longer need access within 1 day.
- Ensure servers and applications not supported by Privia have appropriate security controls.
- Comply with all security controls in the HIPAA Security Rule and Privia's Security Guidance documents.

CONTINUE

## Course Summary

### You should now be able to:

- Protect patient privacy and safeguard PHI with the appropriate controls.
- Provide patients access to their records in a timely manner.
- Reduce the risk of regulatory, reputational, and cybersecurity events.
- Provide Care Centers with tools to assist them with their Privacy & Security Programs.
- Comply with all contractual obligations of our public and private payers.
- Ensure compliance with all applicable laws and regulations.



**Questions? Contact:**

**Lesley Anne M. Durant, Privacy Officer**

[lesleyanne.durant@priviahealth.com](mailto:lesleyanne.durant@priviahealth.com)

**or**

**Paul Shenenberger, Chief Information Security Officer**

[paul.shenenberger@priviahealth.com](mailto:paul.shenenberger@priviahealth.com)

**CONTINUE**

## What's Next?

---

You may now select 'Exit Course' in the corner to return to Privia University to take the knowledge check.