HIPAA 201 | Privacy and Security for Privia Business Associates

2026

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.

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.

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.

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.

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

Covered Entity or Business Associate?

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.

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.

45 CFR § 164.530 - Administrative requirements *

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.

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)

Policy Awareness and Sanctions: Building a Culture of Compliance

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.

Policy Awareness and Sanctions: Building a Culture of Compliance Cont.

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.

Policy Awareness and Sanctions: Building a Culture of Compliance Cont.

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.

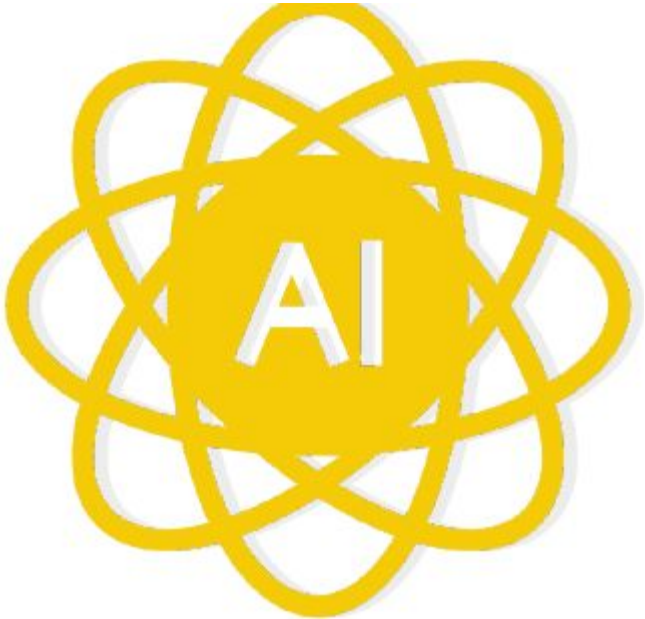
ePHI Access Monitoring: Requirements

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

ePHI Access Monitoring: Artificial Intelligence

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



ePHI Access Monitoring: 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.

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.

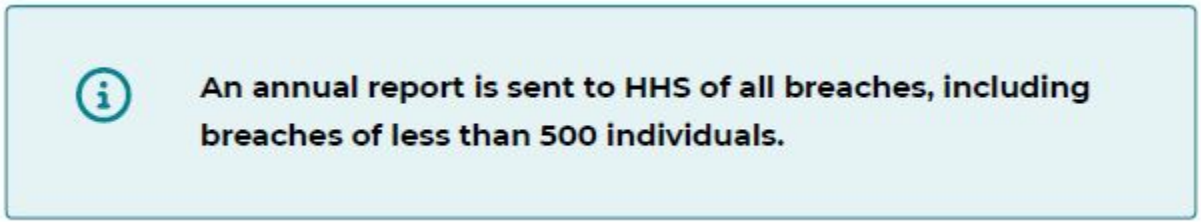
Breach Notification

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



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.

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.

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.

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**.

Examples of Possible Business Associates

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

Examples of Possible Business Associates Cont.

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**.

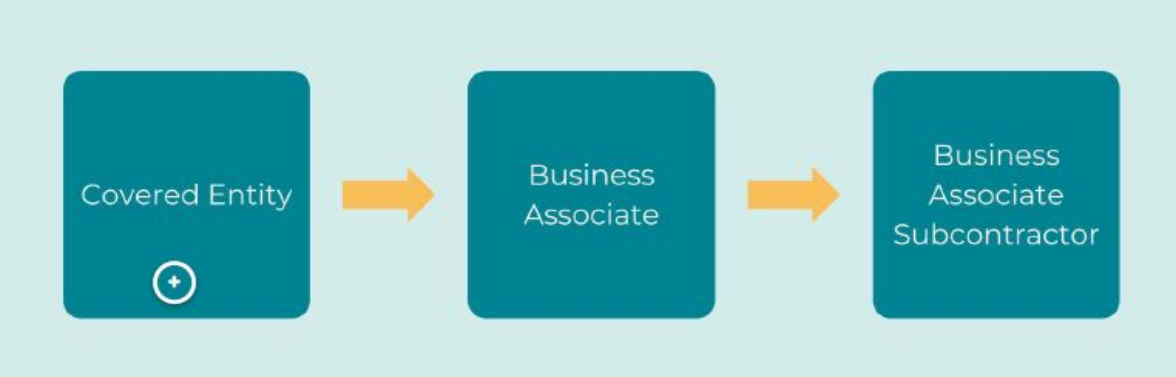
HIPAA Conduit Exception Rule*

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	Not a Conduit
United States Postal Service	Cloud Service Provider
FedEx, UPS, DHL	Online Backup Service
Phone Company	Email Provider
Internet Service Provider	Phone System that records calls

Partnering for Privacy



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.

Partnering for Privacy Cont.

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.

Partnering for Privacy | Business Associate Subcontractor Cont.

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.

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.

Partnering for Privacy | Business Associate Subcontractor Cont.

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.

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.

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

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.

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

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.

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

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

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

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

Business Associate Agreements

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.

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.

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

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.

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.

Completing Your Annual 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.

Completing Your Annual SRA Cont.

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.

Completing Your Annual SRA Cont.

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

Completing Your Annual SRA Cont.

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.

Completing Your Annual SRA Cont.

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.

Completing Your Annual SRA Cont.

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.

Completing Your Annual SRA | 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.

Completing Your Annual SRA | Summary Cont.

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.

Conducting a Comprehensive Annual SRA

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.

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.

HIPAA Enforcement Authority

HHS Enforcement Authority

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:

Affiliated Covered Entities: 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.

Liability for Agents: 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.

Common HIPAA Violations Resulting in Fines for Business Associates

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:

Failure to Conduct a Security Risk Assessment (SRA): Neglecting to perform a comprehensive SRA to identify and address potential vulnerabilities in your systems and 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.

2025 Breach Statistics

- The average cost of a healthcare data breach is **$10.93** million dollars.
- The healthcare industry has the highest cost associated with a data breach for the **13th year** in a row.
- **1/3** of all breaches are identified by an organization's own security teams/tools.
- There has been a **53%** increase in the cost of a healthcare data breach since 2020.
- **82%** of the data involved in breaches is stored in the cloud.
- The average time it takes to recover from a breach is **277** days, 204 days on average to identify the breach and another 73 days to contain the breach.
- **68%** of breaches involve a non-malicious human element.

2025 Tiered Penalty Structure

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

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

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.

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.

Examples of 405(d) Cybersecurity Practices Cont.

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.

Network Management & Firewalls Cont.

- **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.

Privia's Security Guidance Documents (PolicyStat)

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**

Privia's Managed Security 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.

Privia's Managed Security Services Cont.

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.

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.

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.

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.

Privia's Managed Security Services Cont.

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.

Privia's Managed Security Services Cont.

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.

Simplify Your Security

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

Privia's Managed Security Services Cont.

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.

Privia's Managed Security Services Cont.

Privia Managed Tier: Simplified Security for Small to Mid-Size Care Centers 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.

Cybersecurity Protection:

Managed Firewall: 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.

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.

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.

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

or

Paul Shenenberger, Chief Information Security Officer

paul.shenenberger@priviahealth.com