Critical Updates

HIPAA Privacy & Security

2026

2026 Critical Updates | Course Introduction

This course covers the following information related to critical updates in privacy and security:

- Identity Verification
- Responsible AI Use
- AI Vendor Selection
- Contact Information

Critical Updates | HIPAA Privacy & Security

Identity Verification

Critical Security Update: Identity Verification Changes

Because of widespread data breaches, a caller knowing a patient's Name, Date of Birth, and Address is no longer enough to prove who they are. Scammers already have this information. Always take extra steps to verify identity before sharing sensitive information.

1. **Verifying Patients**
    - In Person: Always ask for a Government-issued Photo ID and physically match the face.
    - On the Phone (Ask): Ask for non-public info, like the name of their primary doctor, last appointment date, or a recent medication.
    - On the Phone (Callback): If someone requests sensitive info, hang up and call them back using the phone number already in our system.
2. **Verifying Coworkers & IT**
    - Verify Callers: If "IT" or a "coworker" calls asking for patient data or passwords, do not just give it to them. Hang up and call their internal directory extension.
    - Protect Your Login: Never share your username/password and do not use shared accounts (like "FrontDesk1").

Quick Action Guide

Situation	Required Action
Patient at front desk	Check Photo ID.
Patient calls for results	Ask a chart-specific question (e.g., last visit date) **OR** call them back.
Caller wants portal reset	Send a one-time passcode to the phone/email on file.
Parent asks for child's record	Verify parent's ID and check chart for legal authority.
"IT" calls for a password	**STOP**. Never give passwords. Call the IT extension directly.

Critical Updates | HIPAA Privacy & Security

Responsible AI Use

The Opportunity of AI

Artificial Intelligence has transitioned from a theoretical "science fair project" into a practical tool capable of streamlining operations, reducing administrative burdens, and enhancing the patient experience. While Privia supports efforts to innovate and solve unique healthcare needs, the introduction of AI— especially tools handling Protected Health Information (PHI) or integrating with athenaOne—require a disciplined approach to selection, implementation, and use.

Intelligence should be "Augmented" Not "Artificial"

AI is a tool to support human decision-making, not replace it. Privia's official stance is one of Augmented Intelligence.

The Rule

Technology is used to assist human decision-makers, not to replace them. AI technology provides valuable insights and recommendations, but humans remain at the center of all critical decisions.

Human Accountability

A qualified human professional must always be accountable for any AI-generated output, and outputs must be reviewed and validated on a repetitive and ongoing basis. Responsibility for the accuracy and appropriateness of work cannot be delegated to AI systems.

AI Risks to Watch For

AI Risks to Watch For:

Confabulation (Hallucination): Generative AI can confidently present erroneous or false content. Always verify facts, citations, and logic.

Bias: AI models can amplify historical and societal biases, leading to unfair outcomes for specific demographic groups.

The 8 Core Principles of AI Adoption

All AI usage at our organization must align with these eight ethical pillars defined in our Acceptable Use Policy.

Privacy by Design	Privacy is configured from the start; we do not retroactively "fix" privacy.
Data Minimization	We use only the minimum amount of data necessary to achieve the specific purpose.
Purpose Limitation	Data collected for treatment is not fed into open AI models for undefined training.
Transparency	We should disclose to patients and stakeholders when AI is being used.

The 8 Core Principles of AI Adoption Cont.

All AI usage at our organization must align with these eight ethical pillars defined in our Acceptable Use Policy.

Security	We implement robust measures to protect data from unauthorized access.
Accountability	Clear lines of responsibility are established; humans are accountable for AI outputs.
Fairness	We ensure systems do not perpetuate bias or inequity across populations.
Compliance	We comply with all federal and state laws (e.g., HIPAA, TRAIGA).

Critical Updates | HIPAA Privacy & Security

AI Vendor Selection

The "Shared Responsibility" Model: Who Owns What?

Care centers operating independent businesses on a shared technical platform means safety is a joint effort. It is critical to distinguish between the security of the connection and the accountability for the outcome.

- **Privia's Role**: Privia validates that a vendor is technically secure, will not disrupt the athenaOne EMR, and adheres to general data privacy and security standards through the Third Party Access Committee ("TPAC") Review.
- **Practice Role**: Care centers are the responsible party for the vendor's activity. The Practice is liable for the clinical quality, billing accuracy, and patient consent associated with any tool it deploys.

Where to Begin: Leverage Existing Resources

Before seeking outside vendors, Practices should explore the vetted solutions already available within the Privia and athenahealth ecosystems. Many of these options are included in the Privia management fee.

1. **Internal Resources**: Start by reviewing capabilities on Privia Connect, Privia University, and athena's Success Community.
2. **athena's Product Roadmap**: Available on the Success Community, this helps Practices see "what's next" for athena's native AI innovations.
3. **Approved Vendors**: Check the Privia Savings Guide and the Third-Party Access Committee (TPAC) "Approved Vendor" list.
4. **athena Marketplace**: For solutions requiring athenaOne integration, the Marketplace features vendors designed to work "out of the box."

The 5 "Golden Rules" for AI Selection

Before signing any contract or trial agreement, these items are non-negotiable:

Rule	Requirement	Reasoning
TPAC Approved	Must be vetted by Privia's TPAC Committee.	All tools must have an approved technical integration.
Direct BAA	Vendor signs a BAA with the Care Center or Privia.	The contracting entity must maintain direct legal protection and accountability for HIPAA compliance.
No Data Training	Vendor cannot use Privia PHI to train their models.	PHI must never be used to improve a vendor's product for other customers.
US Residency	Data must be stored and processed in the US.	All PHI must remain on US-based servers to ensure domestic legal and security oversight.
Human in the Lead	Outputs must be reviewed by a person.	A licensed professional must review and sign off on all AI-generated clinical or billing data.

Risk Analysis: What Could Go Wrong?

The "Runaway Coder" (Revenue Risk):

- A practice uses AI to automate billing. The AI "upcodes" visits to higher levels to maximize revenue. During an audit, the provider may be held liable for **False Claims** violations because a physician did not manually review the codes.

The "Invisible Scribe" (Clinical Risk):

- An AI "hallucinates" a medication the patient never took. The doctor signs without reading, and the error becomes part of the permanent medical record.

The "Data Vacuum" (Privacy Risk):

- A low-cost tool uses your patient data to "train" models for other customers. This is an unauthorized use of PHI under HIPAA. **If the product is free, your data is likely the price**.

REMEMBER: The Clinical Licensee is legally responsible for all AI generated outputs related to patient care and claims submission.

Critical Updates | HIPAA Privacy & Security

Contact Information

Contact the Compliance, Privacy, & Information Security Team

Report an Incident or Event	Fastest response for reporting privacy, security, compliance, or ethics events, incidents, or potential breaches. compliance@priviahealth.com
Ask a Question?	**Compliance Team**: compliance@priviahealth.com **Privacy Team**: privacy@priviahealth.com **Security Team**: security@priviahealth.com
Get Support	**Privia Support**: **for Care Center and technical support** **888.774.8428** / www.priviaconnect.com Monday - Friday 8am to 6pm EST
Report Anonymously	**Ethics Line**: **for confidentiality and anonymously report ethics violations** **877.541.9048** / www.priviahealth.com/ethicsline 24 hours a day / 7 days a week / 365 days a year

NOTE: If you choose to report a concern anonymously, please be as thorough and detailed as possible. Providing incomplete information anonymously may limit Privia's ability to investigate.