Critical Updates | Privacy & Security

2025 Critical Updates | Course Introduction

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

- **The Threat Landscape**
- **Regulatory Updates**
- **Payment Card Industry (PCI) Updates**
- **Non-Provider Encounter Sign off Delegation**
- **Emerging Technologies**
- **Protecting Yourself and Your Patients | What You Can Do**

After completing this course, you will have a knowledge check. A score of 100% is required to receive credit for the course.

Continue to Threat Landscape

Threat Landscape

In this section, you will explore the concept of threat landscapes and their significance in cybersecurity. We will examine the various types of threats organizations face, including cyberattacks, data breaches, emerging vulnerabilities, threat actors, phishing, social engineering, ransomware, and the importance of multi-factor authentication (MFA). By the end of this lesson, you will have a clear understanding of how to identify, assess, and mitigate these threats effectively, concluding with strategies to safeguard against them.

Phishing, Scams, & Ransomware

$9.77 million

Industry with the highest average cost of a data breach for the 14th year in a row; 10.6% reduction from 2023.

CONTINUE

2024 Year at a Glance

$$$ Financial Motivation

↑	↑	↑	↓
Insider Threats	**Social Engineering**	**PII (Personally Identifiable Information)**	**Average Breach Cost**

Flip the card below to read more.

Number of patient records exposed in the US since January 1, 2024.

279,963,710

Breached records contained PHI & PII, including: Social Security numbers, phone numbers, medical record numbers, appointment data, billing data, diagnoses, and more.

CONTINUE

Social Engineering Attacks and Scams in 2025

- Powered by AI
- Professional appearance
- Includes realistic fake audio and video (may impersonate you or your colleagues' voices and images)
- Data-driven

CONTINUE

95% of all threat actor activity is financially motivated.

Flip each card below to learn more about what threat actors are seeking:

Personally Identifiable Information (PII)

Threat actors are interested in personally identifiable information (PII) so that they can monetize it or use it to launch attacks.

Credentials

Credentials, such as your username and password, can be used to gain access to systems.

ⓘ **The goal of threat actors is to gain access to your systems and data for extortion.**

CONTINUE

AI-Powered Social Engineering

Click on each "+" below to read more about AI-powered social engineering.

Hyper-Realistic Phishing Emails & Texts

AI generates grammatically correct and highly convincing messages that imitate legitimate communications.

Deepfake Voice Scams (Vishing)

AI can clone voices of trusted individuals (e.g., doctors, clinic staff) to make fraudulent requests sound authentic.

Personalized Attacks at Scale

AI analyzes breached data to tailor scams to individual patient vulnerabilities or recent medical interactions.

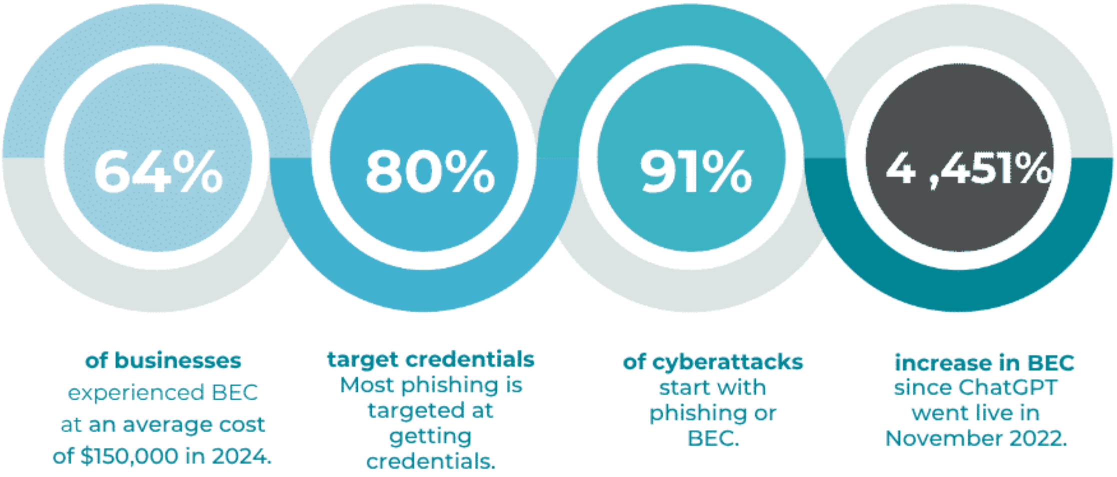
The Challenge: It is more difficult for patients and staff to distinguish between real and fake.

Suspicion should be the default.

Be **skeptical** and **aware** because well over 50% of all emails are not legitimate. With bot traffic, misinformation, fake reviews, and spammy websites, a substantial portion of what you encounter online is not “authentic.”

CONTINUE

Business Email Compromise (BEC) & Phishing



64% **of businesses** experienced BEC at an average cost of $150,000 in 2024.

80% **target credentials** Most phishing is targeted at getting credentials.

91% **of cyberattacks** start with phishing or BEC.

4 ,451% **increase in BEC** since ChatGPT went live in November 2022.

CONTINUE

What is Phishing?

WHAT IT IS	FLAWLESS FAKES	PERSONALIZED PRECISION	ERODING OLD CLUES

- Attempts to steal sensitive information, such as credentials, financial details, or protected health information (PHI), by masquerading as a trusted source in emails, texts (Smishing), or voice calls (Vishing).

- This tactic exploits trust to deceive individuals into sharing private data.

WHAT IT IS | FLAWLESS FAKES | PERSONALIZED PRECISION | ERODING OLD CLUES

- AI-generated scams produce grammatically perfect, contextually relevant, and highly convincing emails or messages.
- These often mimic known brands or internal communications, making them harder to detect.

WHAT IT IS | FLAWLESS FAKES | PERSONALIZED PRECISION | ERODING OLD CLUES

- Scams are increasingly tailored using breached data, such as information from Change Healthcare, to target specific individuals.
- This personalization makes the lures more relevant and effective.

WHAT IT IS | FLAWLESS FAKES | PERSONALIZED PRECISION | ERODING OLD CLUES

- Poor grammar or generic greetings, once reliable indicators of scams, are becoming less common.
- Modern scams are more sophisticated, making traditional warning signs less effective.

How to Identify Phishing

Click each "+" below to read more about signs of phishing.

Unexpected Urgency or Threats

"Immediate action required," "account suspension," and pressure to bypass normal procedures.

Requests for Credentials or Sensitive Data

Never provide passwords, MFA codes, or full SSNs via email or unsolicited calls. For login or information requests, type the official website address into your browser or use a trusted bookmark.

Suspicious Links & Attachments

Hover over links to see the actual destination. Be cautious of unexpected attachments.

Out-of-Character Requests

Does the request align with the sender's typical behavior or responsibilities?

Slight Email Variations

Don't just trust the display name; inspect the full email address.

Look for subtle differences in sender addresses (e.g., jane.doe@privahealth.com vs. jane.doe@priviahealth.com).

Be cautious of homoglyph attacks where characters are replaced by identical-looking ones from different alphabets (e.g., priviahealth.com using a Cyrillic 'a'). These Internationalized Domain Names (IDNs) can be difficult to distinguish from the legitimate domain.

Think Before You Click/Tap

Be inherently skeptical.

Confirm Unusual Requests:

Use a separate, known communication channel (e.g., a phone call to a verified number) to verify unexpected or sensitive requests.

CONTINUE

Ransomware: A Critical Threat

WHAT IT IS | THE "DOUBLE EXTORTION" TACTIC | HOW IT SPREADS

- Ransomware is a type of malicious software that encrypts a victim's files or entire system, rendering them inaccessible.
- Attackers then demand a ransom payment, typically in cryptocurrency, to restore access.

WHAT IT IS | THE "DOUBLE EXTORTION" TACTIC | HOW IT SPREADS

- Many ransomware attacks now involve "double extortion."
- Attackers not only encrypt your data but also steal copies of it before encryption.

- They then threaten to publicly leak the sensitive information if the ransom is not paid, adding immense pressure on victims.

WHAT IT IS

THE "DOUBLE EXTORTION" TACTIC

HOW IT SPREADS

- Ransomware is often delivered through phishing emails, which may contain malicious attachments or links, exploited vulnerabilities in software, or compromised credentials.

Ransomware events are considered Assumed Breaches under HIPAA unless you can prove that data was not exfiltrated.

- Effective Phishing Safeguards
- Workforce Awareness
- Never provide credentials under suspicious circumstances.
- Multi-Factor Authentication (MFA)

CONTINUE

Multi-Factor Authentication (MFA)

WHAT IS MFA?

WHY IS MFA CRUCIAL?

Multi-Factor Authentication is a security measure that requires users to provide two or more verification factors to gain access to a resource, such as an application, online account, or VPN.

WHAT IS MFA?

WHY IS MFA CRUCIAL?

MFA adds a critical layer of security beyond just a username and password. Even if your password is stolen, MFA can prevent unauthorized access because the attacker would still need the additional verification factor(s).

All Privia systems require MFA.

- For systems that you or your Care Center manage, ensure that MFA is enabled for all logins, especially those over the internet.
- Implement robust identity verification procedures for any password resets that you or your Care Center manage.

CONTINUE

Caller ID Spoofing

How it Works: Scammers manipulate caller ID to display our clinic's name or number (or that of a hospital, insurer, or pharmacy).

The Goal: To trick patients into divulging sensitive information (Social Security Numbers, Medicare IDs, financial details, health conditions) or making fraudulent payments.

Patient Impact: Financial loss, medical identity theft, anxiety, and erosion of trust.

> 🚩🚩**Red Flag:** Unexpected calls asking for immediate payment or extensive personal details. **Our staff will rarely ask for full SSN or credit card information over an unsolicited call.**

Ensure that patients understand that Caller ID is **NOT** a security feature. Emphasize that they should hang up and call the published office number if they ever have any concerns.

CONTINUE

Fighting Back and Safeguarding Our Platforms

Privia | We Do

- Privia employees are trained to safeguard against social engineering attacks, including enhanced identity verification procedures for all callers.
- Implementation of MFA for all logins.
- Privia's Managed Google Workspace platform features state-of-the-art anti-phishing and malware detection.
- Free anti-malware tools are available for all Care Centers.

Care Center | You Do

- Ensure that all of your workforce members understand the importance of cybersecurity awareness and best practices.
- For any system you manage, make sure that you have MFA enabled.
- If you do not have Privia's Managed Security Services, ensure that all endpoints have next-generation anti-malware protection and that your email is configured with advanced anti-spam features.

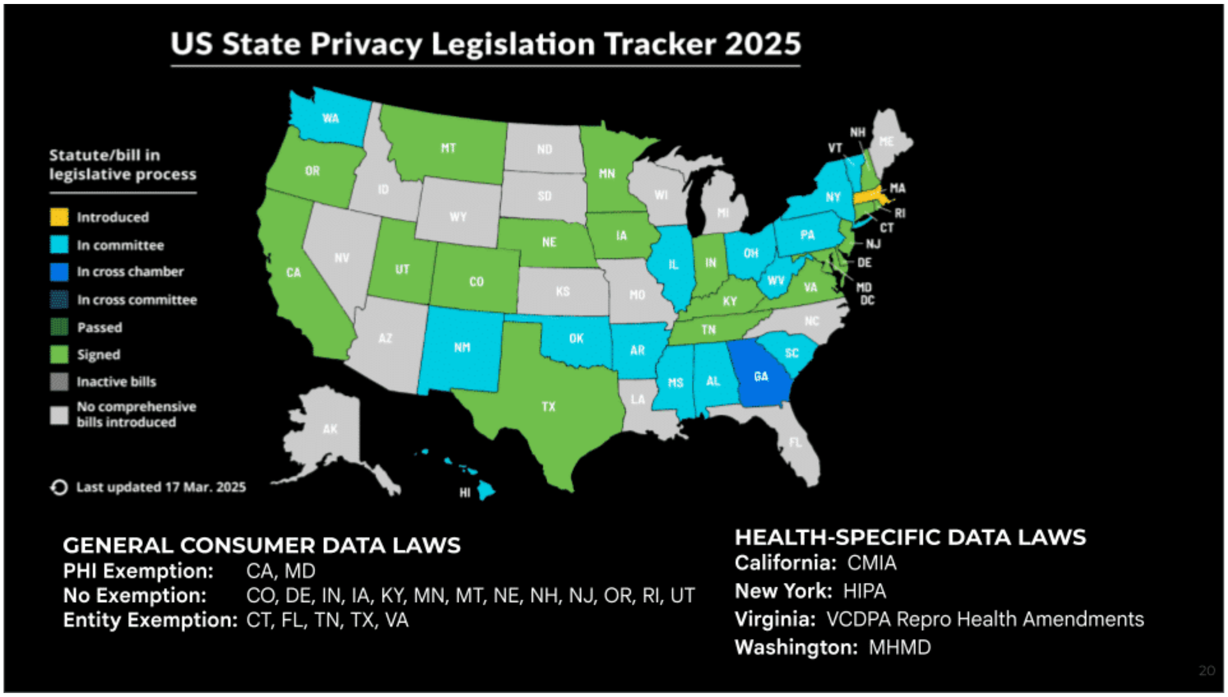
Continue to Regulatory Updates

Regulatory Updates

Staying informed about regulatory updates is essential for compliance and operational success. Updates in this section include new state privacy laws that enhance data protection and a review of patient identification and verification protocols. Understanding these updates ensures organizations remain aligned with legal and industry requirements.

State Privacy Laws: Beyond PHI

- For the first time, **Personally Identifiable Information (PII)** has become the **primary target** for threat actors in healthcare, by a significant margin.
- **Nineteen states** have enacted comprehensive privacy laws regarding PII, with fourteen others having active bills moving through their legislatures.
- State-level momentum for **comprehensive privacy bills** is at an all-time high. This has resulted in a regulatory shift from federal to state and from PHI to PII.
- Additionally, there has been an **exponential increase in class action lawsuits** as a result of this new focus on consumer data privacy.



US State Privacy Legislation Tracker 2025

GENERAL CONSUMER DATA LAWS
PHI Exemption: CA, MD
No Exemption: CO, DE, IN, IA, KY, MN, MT, NE, NH, NJ, OR, RI, UT
Entity Exemption: CT, FL, TN, TX, VA

HEALTH-SPECIFIC DATA LAWS
California: CMIA
New York: HIPA
Virginia: VCDPA Repro Health Amendments
Washington: MHMD

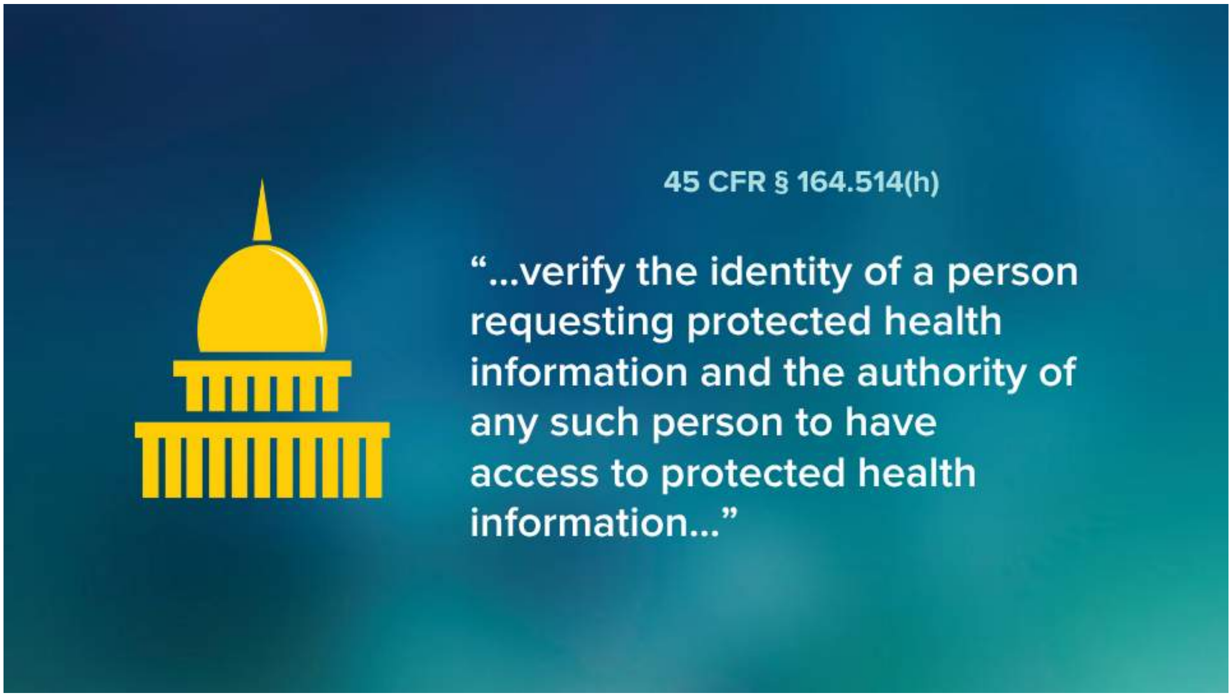
20

It is essential to **review your state's consumer privacy laws** and **ensure that all personally identifiable information (PII) is treated as confidential** and **used in compliance with these regulations.**

This includes: Social Security numbers, phone numbers, IP addresses used for website analytics (such as cookies and pixels), and other sensitive data.

CONTINUE

Medical Record Identity Verification



45 CFR § 164.514(h)

"…verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information…"

https://www.law.cornell.edu/cfr/text/45/164.514

- The identity of a patient **MUST** be verified prior to accessing or assigning a chart to your department.
- Due to the online patient portal and the mailing of billing statements directly from our system, improperly assigned or overwritten charts can lead to a breach of PHI.
- EMR users must follow the best practices outlined in the following section to verify patient identity before registering a patient to a department.

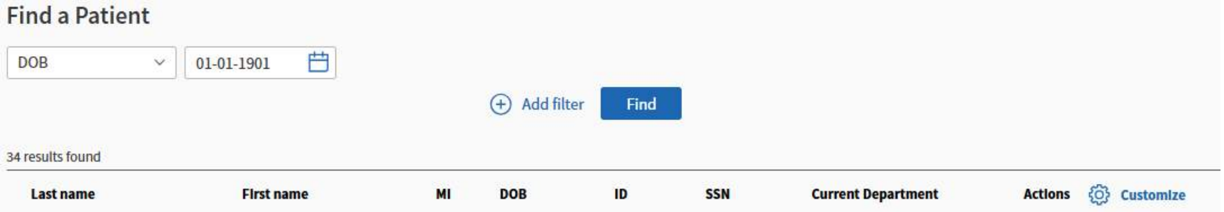
CONTINUE

Patient Search

QUICK SEARCH | ADDITIONAL FILTERS | NEW PATIENTS

When searching for a patient in athenaOne, use date of birth (DOB) or phone number to reduce multiple matches when looking up a patient.

Quick Search: Use the DOB filter.



Find a Patient

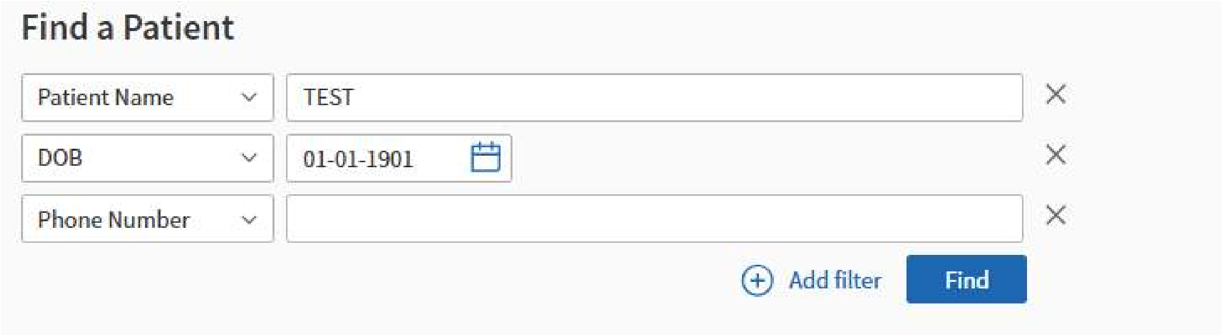
DOB: 01-01-1901

34 results found

Last name	First name	MI	DOB	ID	SSN	Current Department	Actions

QUICK SEARCH | ADDITIONAL FILTERS | NEW PATIENTS

To refine your search further, use additional filters such as Patient Name and Phone number as necessary to find the patient.



Find a Patient

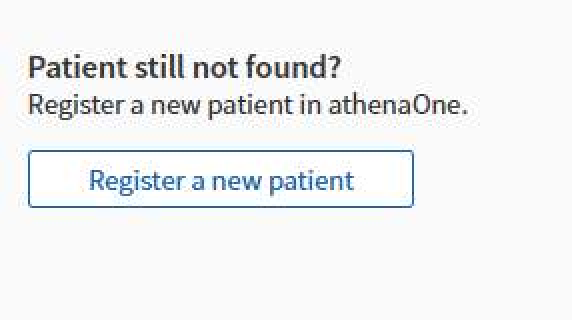
Patient Name: TEST

DOB: 01-01-1901

Phone Number:

QUICK SEARCH | ADDITIONAL FILTERS | NEW PATIENTS

If the patient does not exist in athenaOne, click Register New Patient to create a new record.



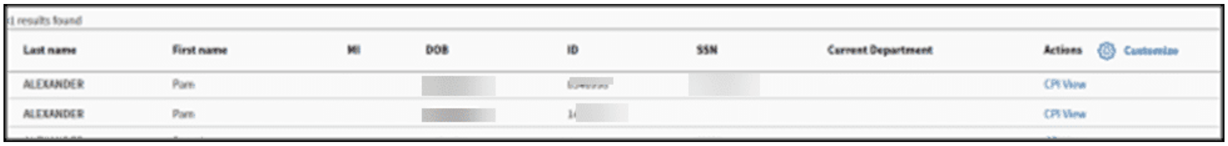
Patient still not found?
Register a new patient in athenaOne.

CONTINUE

Handling Existing Patients - Multiple Results & Verification

PATIENT SEEN ELSEWHERE | HOVER TO ACCESS QUICKVIEW | VERIFY PATIENT ADDRESS

- If your patient has not been seen at your practice, but has visited another provider affiliated with Privia, multiple results may appear in the system.
- Ensure you carefully review the details to identify the correct patient.

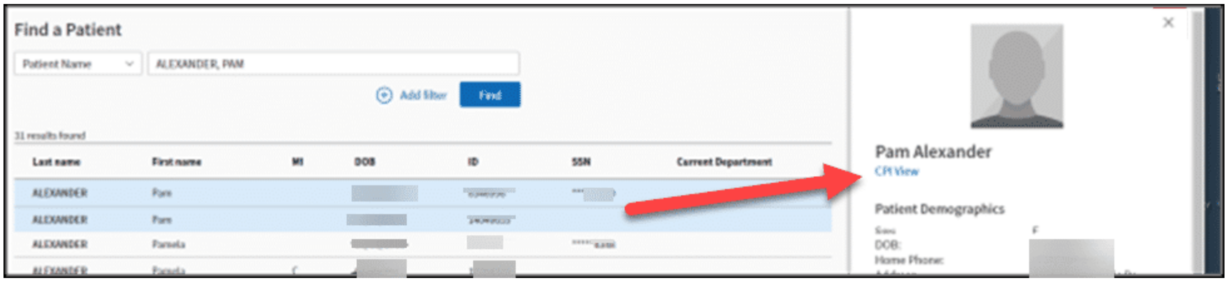


1 results found

Last name	First name	MI	DOB	ID	SSN	Current Department	Actions ⚙ Customize
ALEXANDER	Pam		[redacted]	[redacted]	[redacted]		CPI View
ALEXANDER	Pam		[redacted]	1[redacted]			CPI View

PATIENT SEEN ELSEWHERE | **HOVER TO ACCESS QUICKVIEW** | VERIFY PATIENT ADDRESS

- Hover your mouse over the patient entry until it highlights in blue. This action will enable you to open the patient's Quickview, which appears on the right side of the screen.
- Quickview provides essential details to assist in patient verification.



Find a Patient

Patient Name: ALEXANDER, PAM

31 results found

Last name	First name	MI	DOB	ID	SSN	Current Department
ALEXANDER	Pam		[redacted]	[redacted]	***[redacted]	
ALEXANDER	Pam		[redacted]	[redacted]		
ALEXANDER	Pamela		[redacted]	[redacted]	*****[redacted]	
ALEXANDER	Pamela	C	[redacted]	[redacted]		

Pam Alexander
CPI View

Patient Demographics

Sex: F
DOB:
Home Phone: [redacted]

PATIENT SEEN ELSEWHERE | HOVER TO ACCESS QUICKVIEW | VERIFY PATIENT ADDRESS

- To confirm the correct patient, verify the city and state of the address first. Then, cross-check the full street address for accuracy.
- This step ensures you are working with the correct patient record.

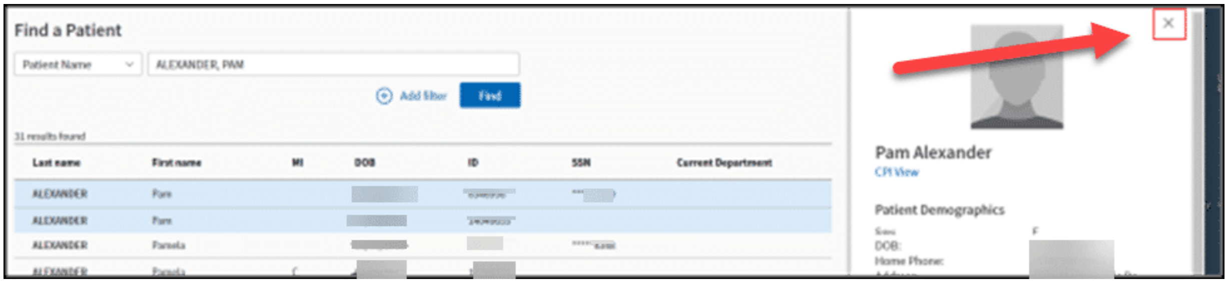
CONTINUE

Registering Patients from Another Care Center (CPI View)

INCORRECT PATIENT SELECTION | REGISTERING AN EXISTING PATIENT | REGISTER EXACT COPY

If the patient you choose isn't the correct patient, click the X at the top right corner of the screen and select another patient.

Do not register the patient into your practice if it's not the patient you are looking for.



Find a Patient

Patient Name ⌄ ALEXANDER, PAM

31 results found

Last name	First name	MI	DOB	ID	SSN	Current Department
ALEXANDER	Pam		[redacted]	[redacted]	[redacted]	
ALEXANDER	Pam		[redacted]	[redacted]		
ALEXANDER	Pamela		[redacted]	[redacted]	[redacted]	
ALEXANDER	Pamela	C	[redacted]	[redacted]		

Pam Alexander

CPI View

Patient Demographics

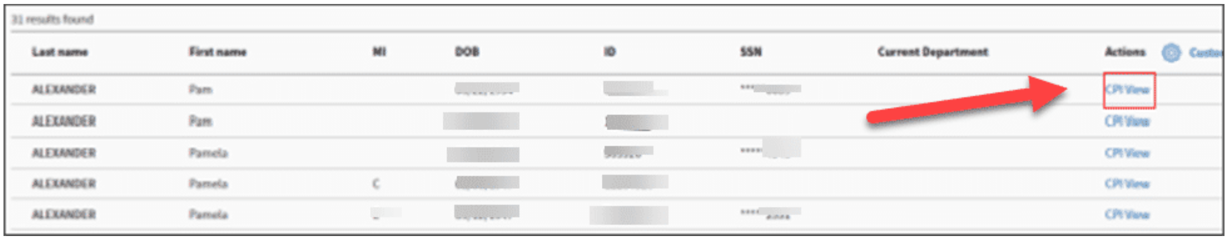
Sex: F
DOB:
Home Phone: [redacted]

INCORRECT PATIENT SELECTION

REGISTERING AN EXISTING PATIENT

REGISTER EXACT COPY

When you find the correct patient, select CPI view. This function allows you to register a patient from another care center into your care center.



31 results found

Last name	First name	MI	DOB	ID	SSN	Current Department	Actions
ALEXANDER	Pam		[redacted]	[redacted]	[redacted]		CPI View
ALEXANDER	Pam		[redacted]	[redacted]			CPI View
ALEXANDER	Pamela		[redacted]	[redacted]	[redacted]		CPI View
ALEXANDER	Pamela	C	[redacted]	[redacted]			CPI View
ALEXANDER	Pamela	[redacted]	[redacted]	[redacted]	[redacted]		CPI View

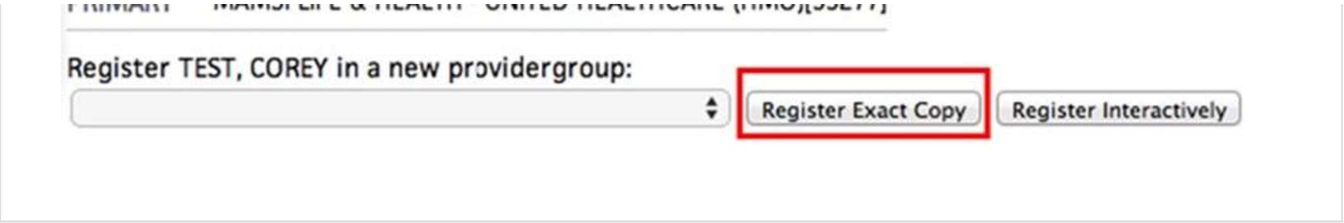
INCORRECT PATIENT SELECTION

REGISTERING AN EXISTING PATIENT

REGISTER EXACT COPY

Go to the bottom of the page and click Register Exact Copy. This action will bring in all the patient demographics and register the patient into your practice.

Take the time to verify the patient's demographics to ensure you have the correct patient.



Register TEST, COREY in a new providergroup:

CONTINUE

Registration Red Flags & Duplicate Chart Management

Important Note: Do not register a patient into your practice and then overwrite all the information in the demographics section!

Registration Red Flags

(Signs of Potential Error):

- Overwriting Name
- Overwriting Date of Birth
- Overwriting legal sex
- Pictures look completely different (if available)

When there is ANY doubt, **register a new patient!**

Duplicate Chart Deletion: To request the deletion of a duplicate or unnecessary patient chart, please email the patient ID numbers to medicalrecords@priviahealth.com

Continue to Payment Card Industry (PCI) Updates

Payment Card Industry (PCI) 4.0

To maintain compliance with PCI, manual credit card entry via keyboard directly into athenaOne is prohibited and has been disabled in athenaOne.

- The only supported devices are Ingenico devices provided by Elavon through athena.
- Ingenico devices can process card-not-present transactions.
- The Privia Call Center has been upgraded to a new PCI-compliant payment system.

Privia Medical Group Policy

[PM.PCI.220.01 Credit Card Payment Processing]

Privia Workflow for athenaOne:

Elimination of Manual Card Entry

Elavon (Payment Processor)

Safe-T P2PE Program

Includes details about skimming, inventory, and incident response

athenaHealth

Credit Card Plus User Guide

PCI Compliance Questions

Krebs on Security

All About Skimmers

Continue to Non-Provider Encounter Sign off Delegation

Non-Provider Encounter Sign off Delegation

ⓘ Delegation of encounter sign-off to non-licensed providers is **highly restricted** and requires strict adherence to CMS guidelines to ensure compliance and prevent potential payor refunds.

Care Center, Provider, and Privia Connect Admin must ensure:

- There is documented approval from the licensed providers for delegation to each individual and the documentation is maintained for six years;
- Delegation is purely for administrative or technical tasks related to documentation after the physician has personally performed and documented the substantive portion of the encounter;
- Non-licensed individuals must not exercise any independent clinical judgment or alter the physician's documented findings, diagnoses, or treatment plan.

May 1 - June 15

Roster Verification Period

Performed annually by Privia Connect Admin during this time frame to ensure accurate user verification.

Starting July 1

Encounter Sign-Off Permission Update

Encounter sign-off permission is removed for all unverified users as part of the verification process.

Compliance & Audit

Encounter Sign-Offs are subject to audit by Compliance for appropriateness. Inappropriate use of clinical encounter sign-off permission may result in refunds to payors.

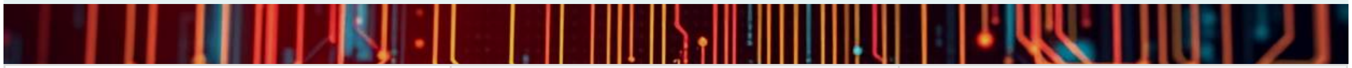
Continue to Emerging Technologies

Emerging Technologies

In this section, you will explore how emerging technologies are transforming industries and reshaping the way we live and work. You will learn about the opportunities and challenges presented by Artificial Intelligence (AI), including the importance of robust guidance to address potential threats. This section also covers innovations in transcription and recording that enhance communication and accessibility, the groundbreaking capabilities of tools like Google Gemini, and the role of consistent Windows updates in maintaining secure and adaptable systems in this fast-paced technological landscape.

Artificial Intelligence Threats

Please click each tab below to read more about artificial intelligence threats:



CYBERSECURITY | PRIVACY | REGULATORY

- AI-powered cyberattacks are becoming increasingly sophisticated, posing significant challenges to security systems.
- The interconnected nature of AI systems has expanded the attack surface, making them more vulnerable to exploitation.
- Additionally, AI models are susceptible to adversarial attacks and data poisoning, which can compromise their integrity and reliability.

CYBERSECURITY | PRIVACY | REGULATORY

- AI models are trained on vast amounts of sensitive data, raising concerns about privacy and data security.
- There is a heightened risk of data breaches, unauthorized access, and re-identification of individuals.
- Ensuring compliance with regulations such as HIPAA is challenging when using AI algorithms, and there is potential for bias in AI systems, leading to discriminatory outcomes.

CYBERSECURITY | PRIVACY | REGULATORY

- The regulatory landscape for AI is evolving, with a lack of specific guidelines creating uncertainty.
- Determining liability and accountability for AI-driven errors remains a significant challenge.
- There is a growing need for transparency and explainability in AI decision-making processes, as well as for robust validation and certification of AI tools, particularly in medical applications.

CONTINUE

Artificial Intelligence Guidance

Click on each tab below for detailed guidance on using AI.

Public AI Chat (ChatGPT)

Limit usage especially sharing confidential data. The consumer model is trained on your data and there are no privacy protections. **NO PHI!**

Image Generation Tools

The image created is generally free to use, however if your prompt uses copyrighted material as a basis you could be subject to copyright claims. These tools frequently have a training bias.

Speech to Text / Text to Speech

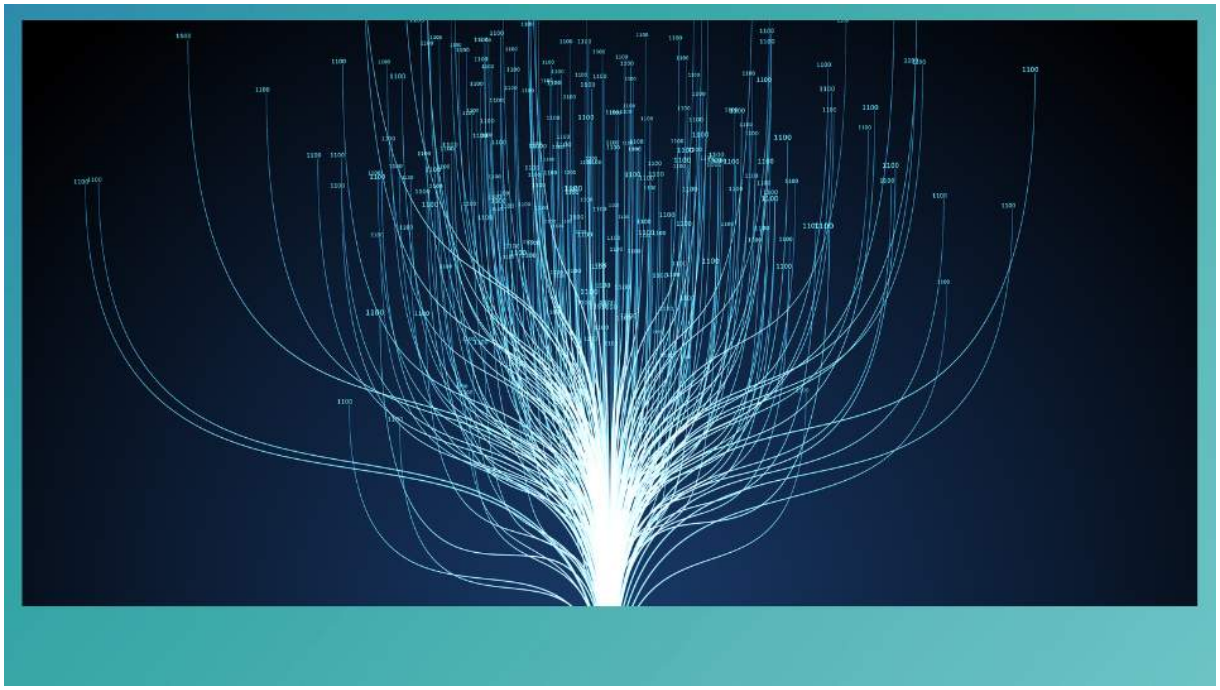
Do not use these tools unless there is a contract, otherwise they are all trained on any data you provide.

AI + PHI = BAA –

Never use an AI tool (or any public website) with PHI or PII without a business associate agreement, NDA, and a commitment to not train with your data.

Privacy and AI Model Training –

Unless there are specific contractual prohibitions assume AI is being trained on the content you feed it.



Hallucinations and Bias

AI do not act like search engines. They create new content based on training data. They may create content that appears factual and is not. **If the training data has bias, the AI has bias!**

CONTINUE

AI Transcription and Recording

- Care Centers should be **very careful** when using recording or transcription technology, **including AI notetakers.**
- A Business Associate Agreement with the recording or transcription services is **REQUIRED** if **any PHI is going to be discussed** on a call.
- Agreements with these applications should also **outline what the vendor is permitted to do** with the information it collects, including using data to train machine learning applications.
- Discussion of PHI on a call with a non-BA application could be considered a **HIPAA breach** and should be **reported to the Privacy Officer** as soon as possible.

CONTINUE

AI for Privia Managed Google Workspace Customers | Gemini

Included with license

There are no additional costs, it is native to Google workspace.

Private and Secure

It is covered by BAA and model is not trained on your data.

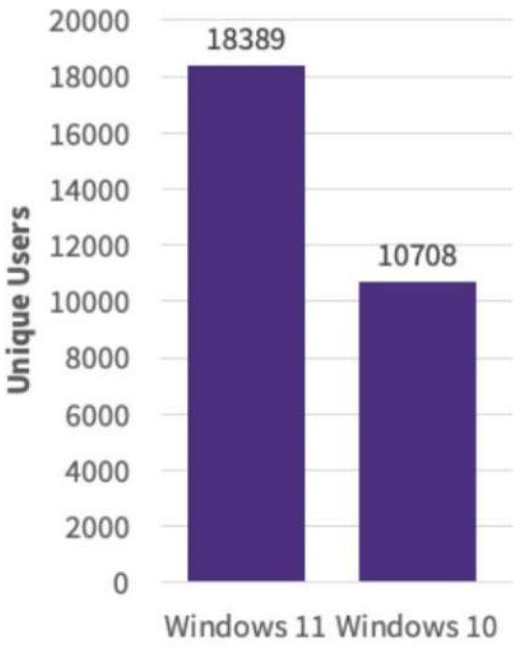
Transcripts & Notetaking

Google Meet has native AI note taking transcription.

CONTINUE

Windows 10

End of Support: October 14, 2025



45 CFR §164.308 (a)(5)(ii)(B)

All software including operating systems must receive regular security updates from the manufacturer to remain HIPAA compliant.

Windows 11 has strict hardware requirements:

- 8th Generation Intel CPU or higher (August 2017)
- TPM 2.0

https://www.microsoft.com/en-us/windows/windows-11-specifications

---

Privia provides Windows 11 compliant computers:

- ✅ Competitive Pricing
- ✅ 3 Year Warranty
- ✅ Endpoint Protection for the Life of the Device (for Supported and Managed Care Centers)

Request a Quote

🖥️

Desktop and laptop supply is expected to be disrupted by tariffs and have highly variable pricing.

Request a Quote for Windows 11:

https://pmg.tfaforms.net/4620197

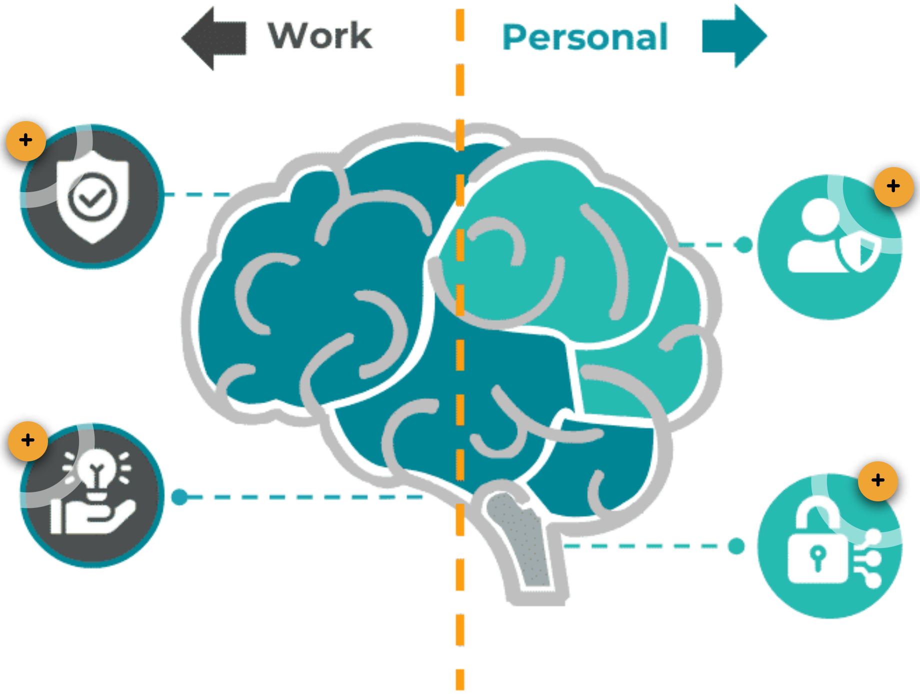
Continue to Protecting Yourself and Your Patients | What You Can Do

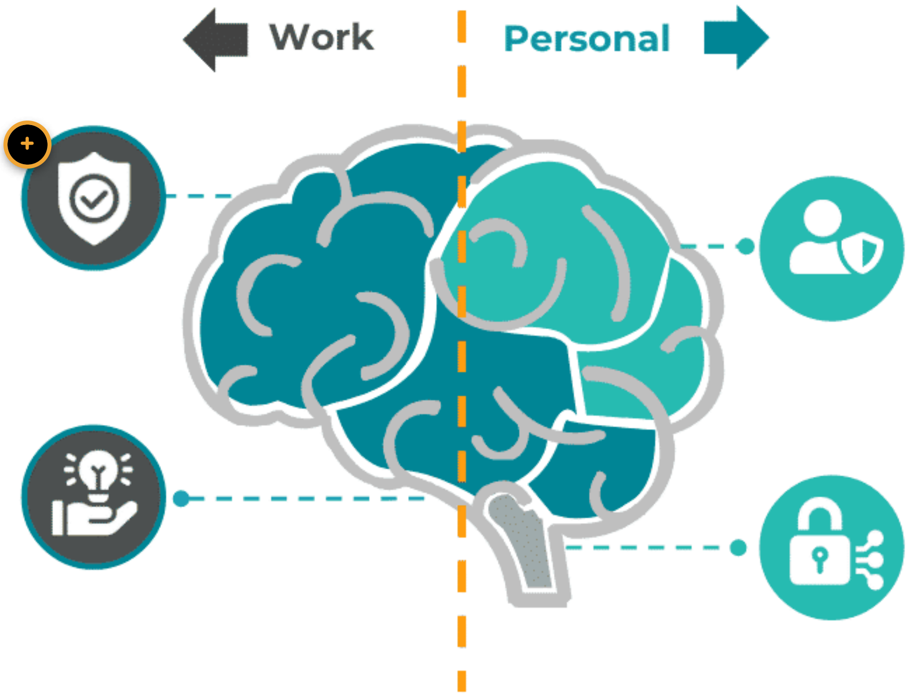
Protecting Yourself and Your Patients | What You Can Do

In this section, you will learn how to maintain a clear boundary between your personal and professional digital activities to safeguard both yourself and your patients. You will explore strategies for minimizing risks such as accidental data breaches, ensuring secure access to sensitive patient information, and upholding privacy regulations. Additionally, this section will guide you on how to communicate with patients about recognizing scams and provide tools like self-service password reset options to enhance security and convenience.

Keeping Your Digital Lives Separate

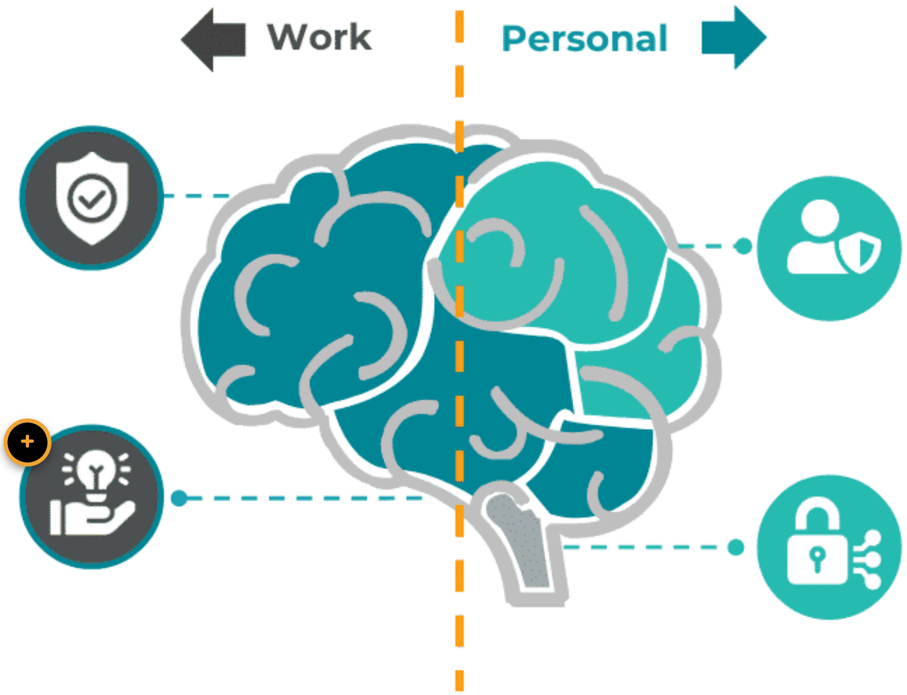
Click on each marker (+) below to read more.





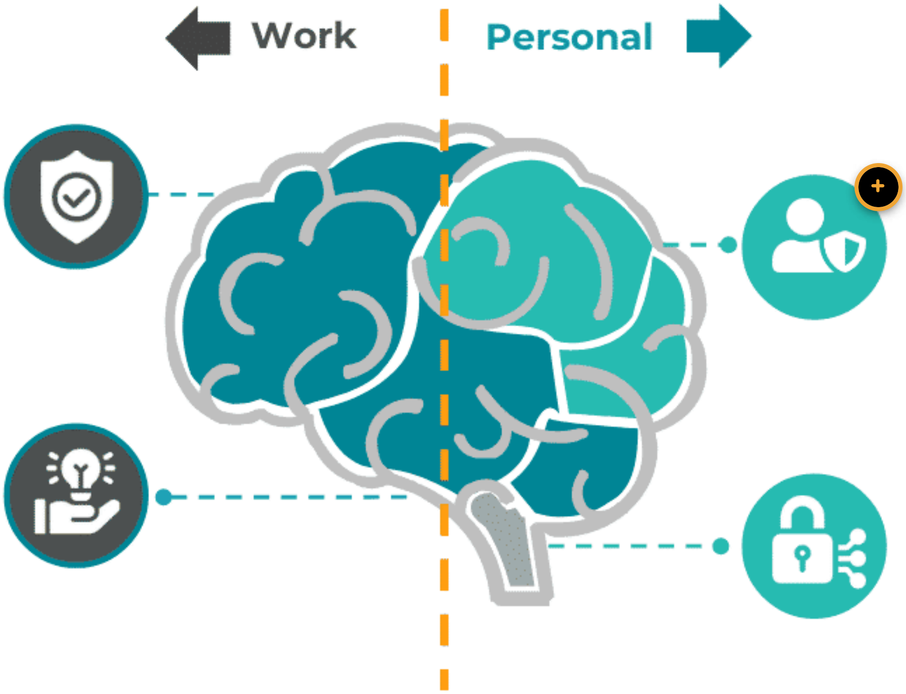
Security Risks

Confidential Information, PHI, and PII should never be stored in personal cloud services (including notes) when mixing accounts it is easier to inadvertently share data with your personal Google Drive, iCloud, OneDrive, etc.



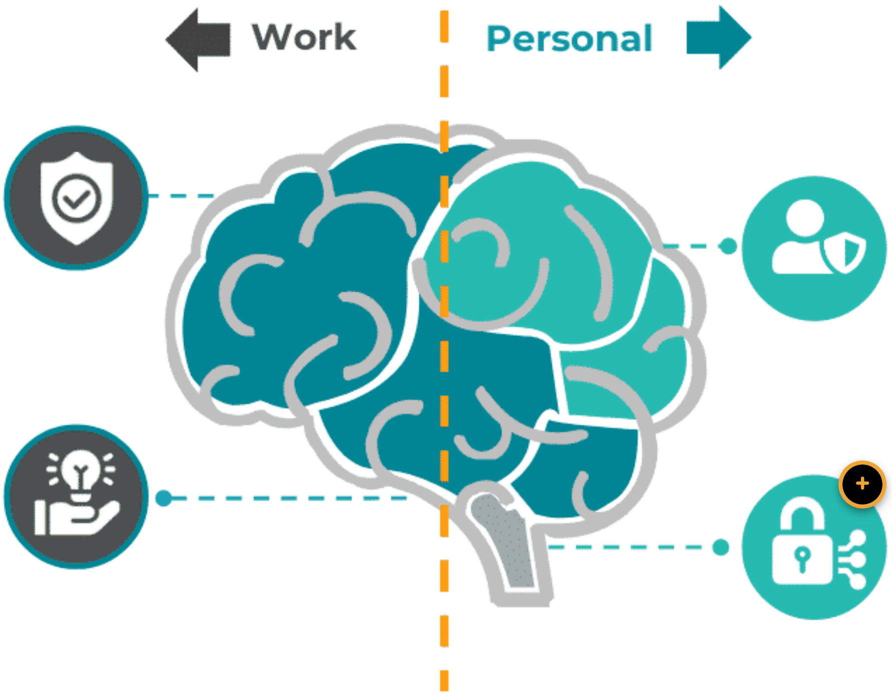
Best Practices

- Don't Use Privia or Care Center email for personal services.
- Don’t synchronize photos or files from iCloud, OneDrive, or personal Google My Drive to your work owned laptop.



Your Privacy Matters

Syncing your personal Apple ID, Google account or OneDrive to a Privia owned laptop could inadvertently share personal photos, iMessages/texts, browsing history, contacts, personal files or app usage with the company's IT systems or seen during IT support.

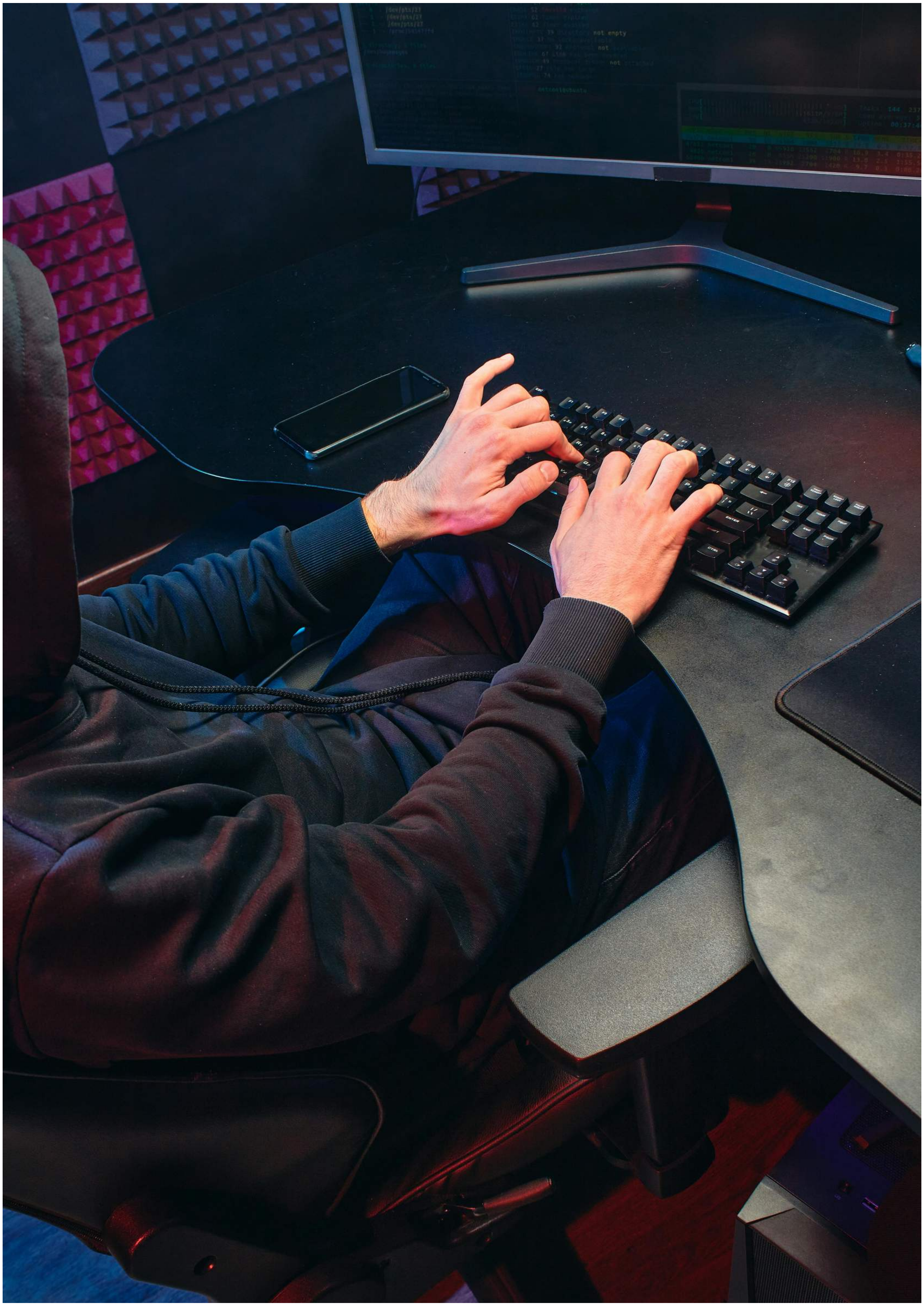


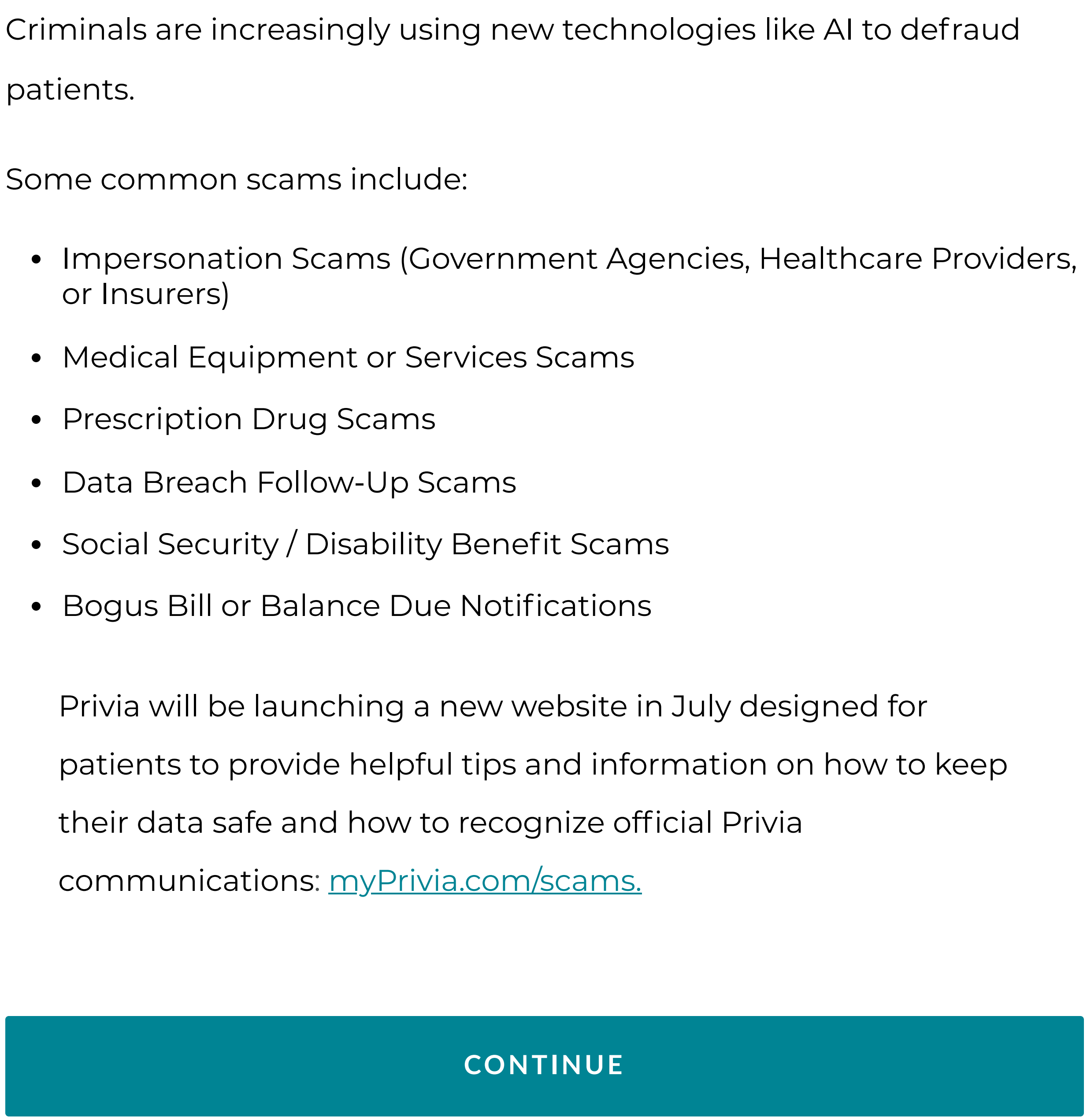
Retain your data!

When you leave the contents of your shared drives stay with your company and personal files may be lost. Your manager may request your email for continuity and continue to get personal emails for services where you use your Privia or Care Center email account.

CONTINUE

Patient Communication on Scams





Criminals are increasingly using new technologies like AI to defraud patients.

Some common scams include:

- Impersonation Scams (Government Agencies, Healthcare Providers, or Insurers)
- Medical Equipment or Services Scams
- Prescription Drug Scams
- Data Breach Follow-Up Scams
- Social Security / Disability Benefit Scams
- Bogus Bill or Balance Due Notifications

Privia will be launching a new website in July designed for patients to provide helpful tips and information on how to keep their data safe and how to recognize official Privia communications: myPrivia.com/scams.

Identity Verification for Password Reset

If you are not able to verify, your manager or Privia Connect Admin will be required to verify your identity.

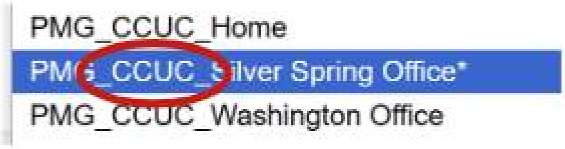
Due to increased attempts to steal credentials through service desks, if you are unable to complete self-service recovery, at least **one (1) proprietary identifier and four (4)** standard identifiers for a minimum of **five (5)** identifiers will be required for account access, password resets, changes to MFA (including EPCS) when contacting the service desk.

CARE CENTER PROPRIETARY | PRIVIA HEALTH PROPRIETARY | STANDARD IDENTIFIERS

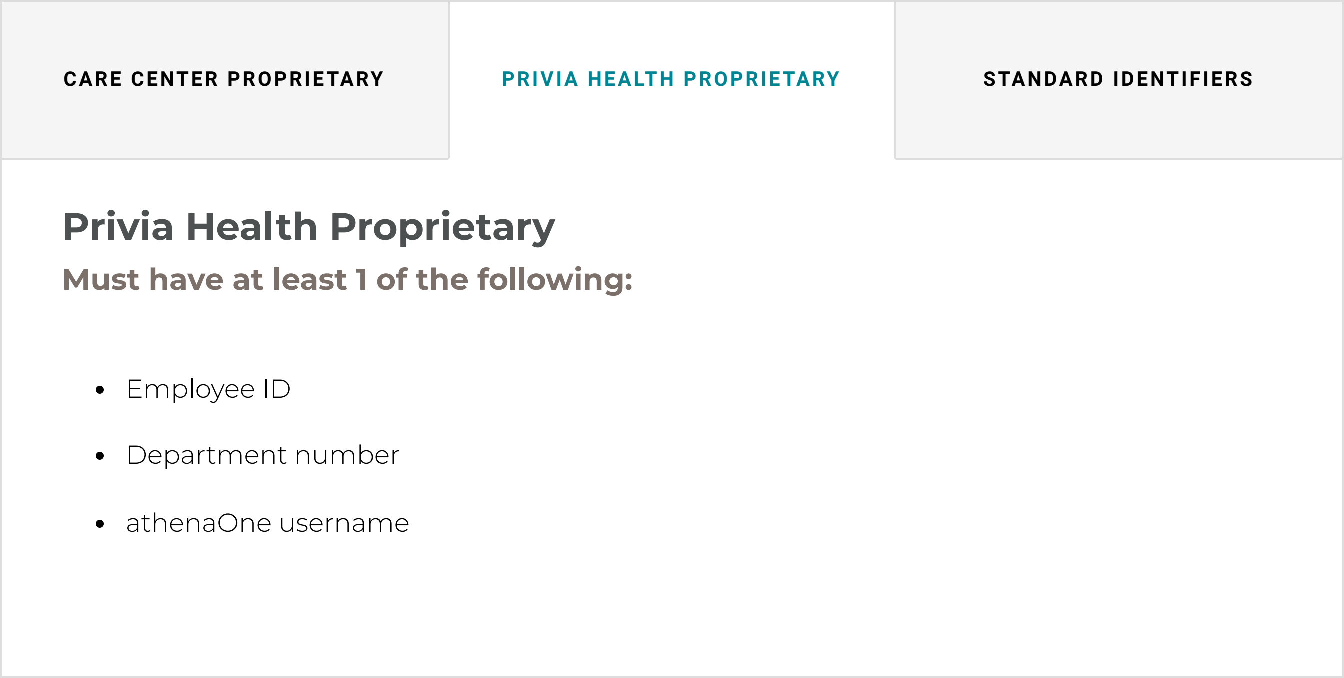
Care Center Proprietary

Must have at least 1 of the following:

- athenaOne username
- Privia.one ID
- athena department name or acronym (circled part below)



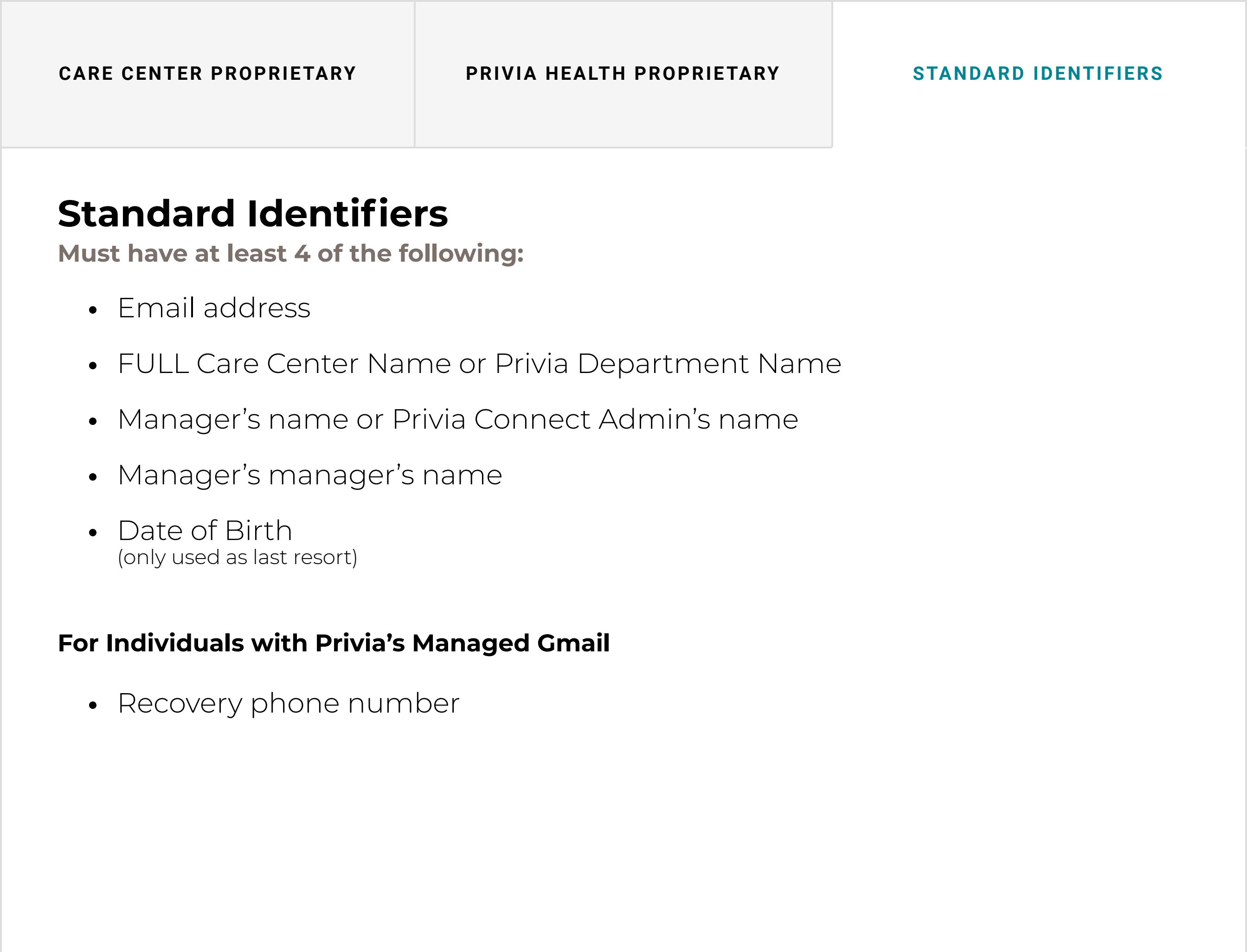
PMG_CCUC_Home
PMG_CCUC_Silver Spring Office*
PMG_CCUC_Washington Office



Privia Health Proprietary

Must have at least 1 of the following:

- Employee ID
- Department number
- athenaOne username



Standard Identifiers

Must have at least 4 of the following:

- Email address
- FULL Care Center Name or Privia Department Name
- Manager’s name or Privia Connect Admin’s name
- Manager’s manager’s name
- Date of Birth
  (only used as last resort)

For Individuals with Privia’s Managed Gmail

- Recovery phone number

- Recovery email address

CONTINUE

Self Service Password Reset

Self Service Password Reset

You can save time and increase security by updating your self service password reset questions and your Recovery Email / Phone

2

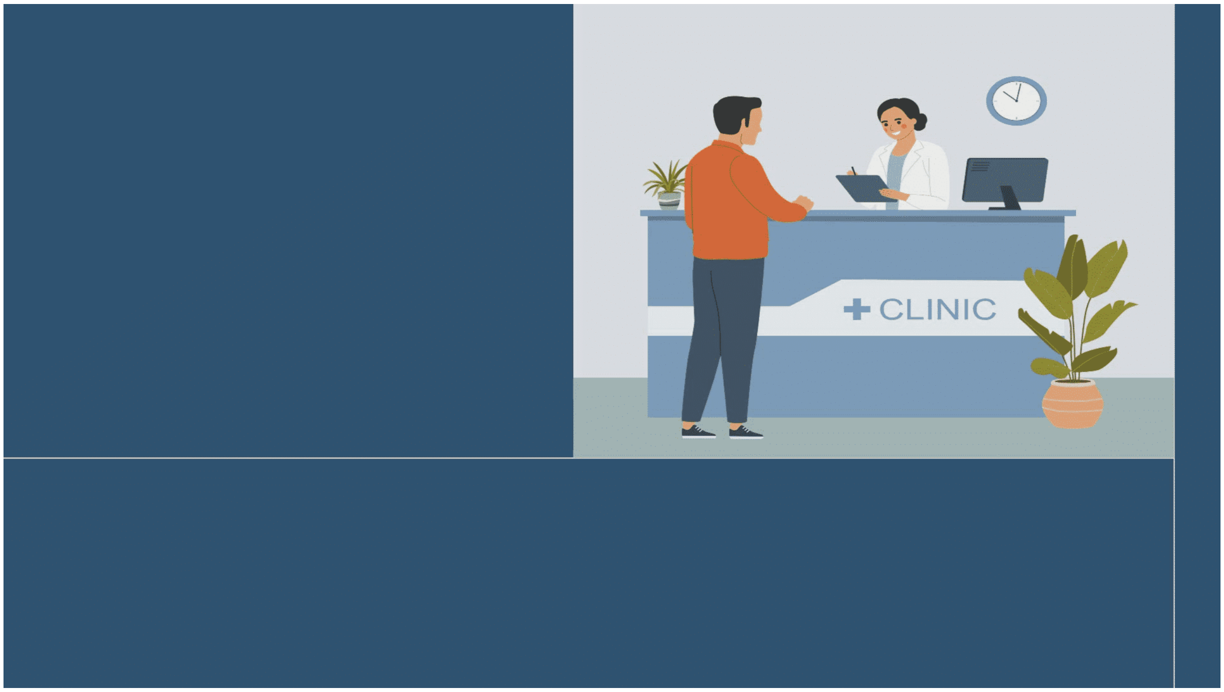
Google/ privia.one

1. Go to your Google Account **myaccount.google.com**
2. Click on **Personal info** in the left navigation panel.
3. Under Contact info, click **Email** (and/or Phone).
4. Under **Recovery email** (and/or Phone), click on your current recovery address (you may need to sign in).
5. Enter the new **recovery email address** (and/or phone) and follow the instructions to verify it.

https://support.google.com/a/answer/3033063

3

Self Service Password Reset for Privia One



You can watch the video above to see the steps.

4

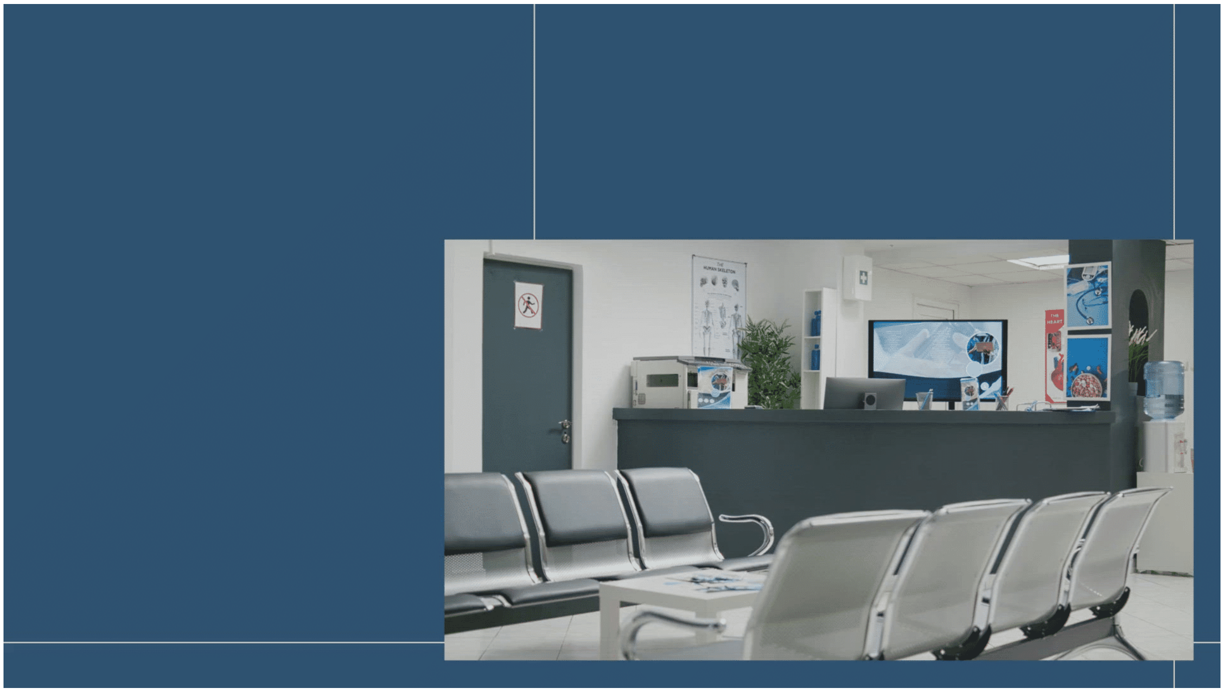
athenaOne

1. Navigate to *User Profile* page:
   Settings (gear icon) > **User Profile.**
2. Click **Security Questions** tab.
3. Make the necessary changes.
4. Enter your <**athenaOne password**> in *Current Password* field.
5. Click **Save.**

https://success.athenahealth.com/s/article/000013486

5

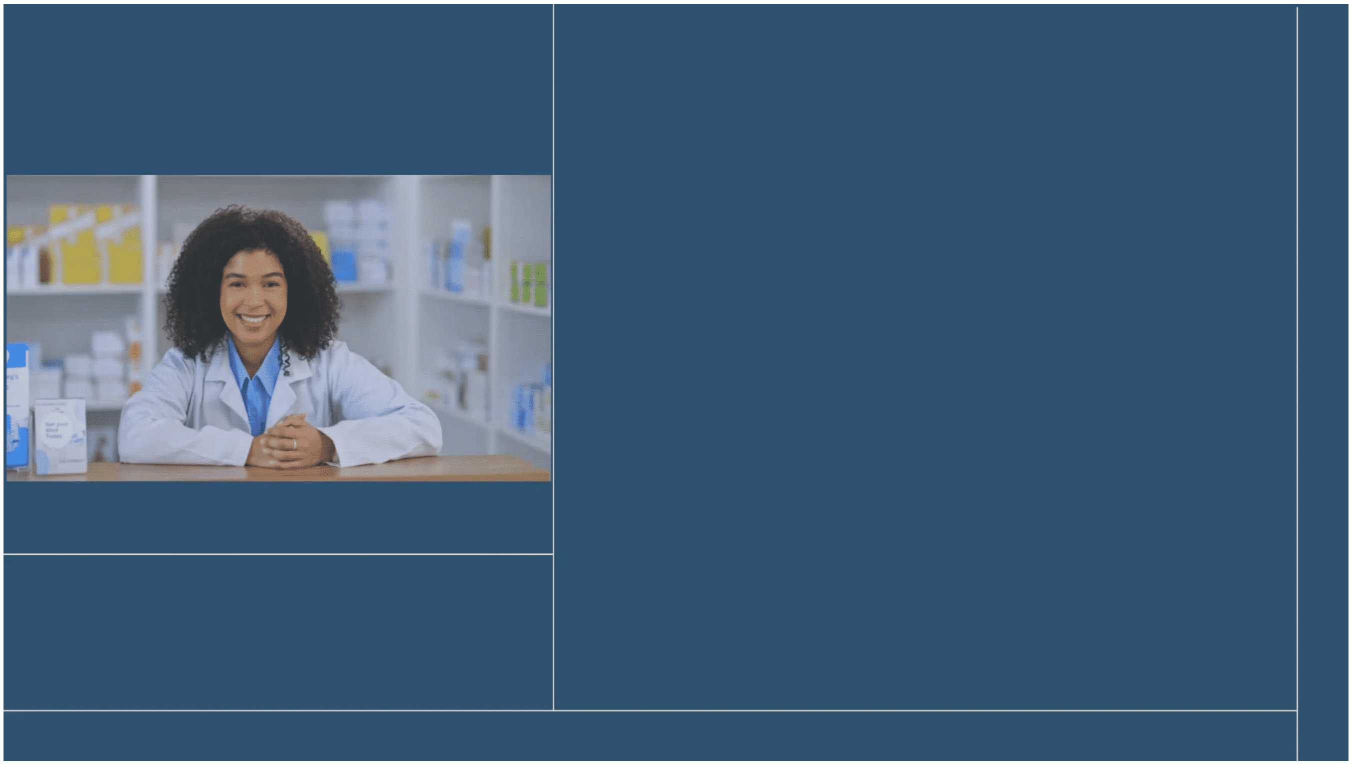
Self Service Password Reset for athenaOne



You can watch the video above to see the steps.

Other Quick Things You Can Do To Help With Security

How to Clear Saved Passwords in Google Chrome



Update Password Security Questions

Continue to Review and Contact Information

Review and Contact Information

Reminders

EVERYONE | COMPLIANCE LIAISON | CARE CENTER LEADERSHIP

- Stay **alert**, and be **suspicious.**
- Don’t hesitate to **escalate**!
  - If it seems wrong a couple of extra minutes is less costly than a threat actor gaining access.
- **Remember your identifiers** and use Self-Service password reset.

EVERYONE | COMPLIANCE LIAISON | CARE CENTER LEADERSHIP

- Users are added and **REMOVED** from the roster timely.
- All individuals that need encounter sign off must have a valid reason, approved by the provider and verified on the roster.

- You have identity verification procedures in place.

EVERYONE | COMPLIANCE LIAISON | CARE CENTER LEADERSHIP

- Upgrade **all** computers to Windows 11.
- Ensure **all** systems not managed by Privia have MFA.
- If you do not use Privia Managed Security Services verify that:
    - **All** systems have next-gen anti-malware.
    - Email is configured with MFA, advanced anti-spam and anti-malware protection.

CONTINUE

Contact the Compliance, Privacy, and 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

*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.

Continue to Knowledge Check

Section 9 of 10

Knowledge Check

You will now answer a few questions about the Critical Updates for 2025. You must score 100% to get credit for this course, you will have multiple attempts to complete this knowledge check. You may to return to the course as necessary to review information.

Question

01/07

Which method is NOT mentioned in the sources as a way AI is used in social engineering attacks?

○ Making phishing emails seem very real and correct

○ Creating fake voices of trusted people for scams

○ Making attacks more personal by using stolen information

○ Stealing hardware from offices

Question

02/07

Are poor grammar or generic greetings still the best way to tell if an email is a scam?

○ Yes

○ No

Question

03/07

What is suggested as a key defense against phishing and online scams?

○ Always trust emails from people you know.

○ Click on links in suspicious emails to see where they go.

○ Be skeptical of what you see online and verify requests through another method you know is real.

○ Share your login details if asked by email to verify your identity.

Question

04/07

Why is Multi-Factor Authentication (MFA) important according to the sources?

○ It makes passwords shorter and easier to remember.

○ It means you never need a password.

○ It is only needed for email accounts.

○ It adds an extra step to log in, which helps stop someone from getting in even if they have your password.

Question

05/07

Once you have set up your recovery email, phone number, and security questions, what is the fastest way to reset your password?

○ Call the Service Desk

○ Use self-service password reset functionality in Google and athena

Question

06/07

What must you do regarding patient identity before accessing or assigning a patient chart to your department?

○ Verification is a good idea but not required.

○ Verification is only needed for new patients.

○ You can verify identity later if you are busy.

○ The patient's identity MUST be verified.

Question

07/07

True or False: Typing credit card numbers directly into athenaOne using the keyboard is allowed for PCI compliance.

○ False

○ True

You may now exit the course.