

PhyCentra — A Product and Service Operated by Folley Healthcare Technologies LLC

PRIVACY POLICY

Consumer-Facing Mobile & Web Application

Effective Date: July 30, 2026

Last Updated: July 30, 2026

Version 1.0

Platform: PhyCentra mobile and web applications.

1. Introduction

PhyCentra is a product and service operated by Folley Healthcare Technologies LLC ("PhyCentra," "we," "us," or "our"). We are committed to protecting the privacy of our users. This Privacy Policy explains what information we collect, how we use it, how we store and protect it, and your rights with respect to your personal information when you use the PhyCentra mobile application (the "Application").

By creating an account and using the Application, you agree to the collection and use of your information as described in this Privacy Policy. If you do not agree, please do not use the Application.

This Privacy Policy applies to the PhyCentra mobile application for iOS and Android and the PhyCentra web application (collectively, the "Application"). It does not apply to any third-party websites, services, or applications that may be linked from within the Application.

2. Information We Collect

2.1 Information You Provide Directly

When you create an account and use the Application, you provide us with the following information:

- Account registration information: first name, last name, middle name (optional), phone number, and email address.
- Professional information: medical specialty, state(s) of licensure, and National Provider Identifier (NPI) (optional).
- Uploaded documents (professional credential documents): state medical license (front required; back optional), DEA registration certificate, board certification records, continuing medical education (CME) certificates, and malpractice insurance documents.

2.2 Information Extracted from Your Documents

When you upload documents to the Application, we use optical character recognition (OCR) technology powered by Amazon Textract, a service of Amazon Web Services, to extract information from those documents. This may include:

- State medical license: name, license number, issuing state, issue date, expiration date, and license status.
- DEA registration: registrant name, DEA number, registered address, schedules authorized, and expiration date.
- Board certification: certifying board name, certification date, and Maintenance of Certification (MOC) or expiration date.
- CME certificates: course or activity name, completion date, and credit hours.

- Malpractice insurance documents: carrier name, policy number, policy period, policy expiration date, and coverage limits, where present. We do not extract, store, or summarize individual claim details, allegations, or claim-related patient information.

OCR extraction is used solely to populate your Credential Readiness Dashboard and generate reminders. OCR and automated extraction features may be incomplete or inaccurate. You are responsible for reviewing and correcting all extracted information, including expiration dates, license numbers, document types, CME hours, DEA information, and reminder settings before relying on them.

We treat DEA registration numbers, medical license numbers, and other professional registration identifiers as sensitive professional information. Access to this information within our systems is restricted to authorized personnel and systems that require it to provide the service, and it is protected by the security controls described in Section 6.

2.3 Information from Public or Third-Party Sources

At this time, the Application does not retrieve or incorporate information from state medical board databases, the DEA, ABMS or its member boards, the National Practitioner Data Bank (NPDB), or any other public licensing or credentialing data source. All credential information reflected in the Application is derived solely from documents you upload.

2.4 Device and Session Data

We collect limited technical information necessary to operate the Application, including:

- Authentication tokens (JSON Web Tokens and refresh tokens) for session management. Tokens expire automatically and are revoked upon logout.
- Push notification tokens to deliver credential reminders and alerts to your device.
- A biometric preference flag (enabled or disabled) stored on our servers. No biometric data itself — including fingerprints or facial scans — is collected or stored by PhyCentra. All biometric authentication is handled entirely by your device operating system using Face ID, Touch ID, or fingerprint recognition.

We do not collect GPS or device location data. We do not use advertising SDKs or sell behavioral data. We may collect limited diagnostic, security, and performance information necessary to operate, secure, troubleshoot, and improve the Application. We do not use this information for advertising or third-party profiling.

2.5 No Patient Information

PhyCentra is designed only for professional credential, licensing, certification, and career-readiness documents. PhyCentra is not intended to store patient medical records, patient-identifiable information, or protected health information. You agree not to upload patient medical records, protected health information, or patient-identifiable information to the Application. Users are responsible for removing or redacting any patient-identifiable information before uploading documents, including from malpractice claim documents, hospital forms, or other records that may contain patient identifiers. If you believe you uploaded patient information by mistake, contact us immediately.

PhyCentra may remove, delete, restrict, or refuse to process any document that appears to contain patient medical records, protected health information, or other prohibited information, with or without notice.

PhyCentra is not designed or intended to be used to store, transmit, or manage patient medical records or protected health information. The current version of PhyCentra is not intended to create a HIPAA business associate relationship between PhyCentra and any user, medical practice, hospital, health plan, or other covered entity, and PhyCentra does not enter into Business Associate Agreements for the current version of the Application unless

separately agreed in writing. Users must not upload PHI or patient-identifiable information unless PhyCentra has separately entered into a written agreement expressly permitting such use.

3. How We Use Your Information

We use the information we collect solely to provide and improve the PhyCentra service. Specifically, we use your information to:

- Create and manage your account.
- Process and store uploaded documents securely.
- Extract credential-relevant data from your documents using OCR.
- Generate your Credential Readiness Dashboard, status indicators, and Credential Readiness Score.
- Send you reminders and alerts about license, DEA, board certification, and CME expirations and other renewal deadlines.
- Authenticate your identity using one-time passcodes (OTP) sent to your registered email address.
- Maintain session security and application performance.
- Generate credential readiness packets at your request, for your own use in employment, privileging, or licensure applications.

We do not use your information for advertising, third-party profiling, credit decisions, insurance underwriting, employment decisions, credentialing determinations, or automated decisions that produce legal or similarly significant effects, or for any purpose other than providing you with the PhyCentra service. We do not use your uploaded documents, OCR outputs, credential information, or personal data to train third-party artificial intelligence models. PhyCentra does not guarantee that reminders, alerts, or notifications will be delivered, timely, accurate, or sufficient to prevent expiration, lapse, missed deadlines, or noncompliance.

PhyCentra is currently offered free of charge. We do not currently collect payment card information or billing information through the Application.

4. Credential Readiness Score — Important Disclaimer

The Credential Readiness Score generated by the Application is an internal, informational indicator based solely on data you have uploaded. It reflects document completeness, expiration timelines, and renewal status as tracked within the Application. The Credential Readiness Score is:

- Not a credentialing determination, licensure status, or risk assessment of any kind.
- Not shared with any third party, including employers, hospitals, credentialing bodies, or licensing boards, unless you affirmatively choose to export and share a credential readiness packet.
- Not used or intended for any eligibility, privileging, underwriting, or employment determination by PhyCentra.
- Informational only and intended solely for your personal awareness and credential management.

PhyCentra does not operate as a credentials verification organization (CVO). The Application does not perform primary source verification and does not access official records from any state medical board, the DEA, ABMS or its member boards, or the NPDB.

5. How We Share Your Information

PhyCentra does not sell your personal information. We do not share your personal information with advertisers or data brokers. We do not share your licensure, certification, or credential information with employers, hospitals, insurers, credentialing bodies, or government agencies, except where you affirmatively initiate an export or share action within the Application.

We share limited information with the following service providers solely to operate the Application:

- Supabase: authentication, database (Postgres), file storage, and backend logic (Edge Functions). Supabase infrastructure is hosted on Amazon Web Services in the United States.
- Amazon Web Services (Amazon Textract): optical character recognition and document data extraction.
- Resend: delivery of one-time passcodes (OTP), verification emails, passwordless authentication emails, and other transactional communications.
- Apple Push Notification service (APNs) and Firebase Cloud Messaging (FCM): delivery of push notifications to iOS and Android devices, respectively.

Each of these providers processes data on our behalf to deliver the specific function described above, under contractual terms that restrict their use of your information, and none of them has independent rights to use your information for their own purposes.

If you choose to export, download, or share a credential readiness packet, you are responsible for ensuring that the recipient is correct and authorized to receive the information. PhyCentra cannot control, retrieve, or delete copies of documents once they have been downloaded, saved, forwarded, or otherwise retained by a recipient.

The web application allows you to share credential readiness packets through secure share links. Shared credential packets automatically expire 30 days after the share link is created unless revoked earlier by you, and you may revoke an active share link at any time through the Application. We log access to shared credential packets, including the date and time a shared link is opened, for security and audit purposes. Revoking or expiring a link prevents future access through that link but does not retrieve copies already viewed, downloaded, or retained by a recipient. Anyone with an active share link may be able to access the shared packet, so you are responsible for sharing links only with intended recipients and through secure channels.

We may disclose your information if required to do so by law, court order, or valid legal process, or to protect the rights, safety, or property of PhyCentra or its users.

6. Data Storage and Security

Your documents and account data are stored in the United States on infrastructure operated by the providers identified in Section 5, principally Supabase, whose platform is hosted on Amazon Web Services. The Application is intended for use in the United States. If you access the Application from outside the United States, you understand that your information will be processed and stored in the United States. We implement the following security controls:

- Encrypted storage for all documents and personal data.
- Secure API communications using industry-standard encryption protocols.
- Access controls limiting data access to authorized personnel.
- Passwordless authentication using one-time passcodes (OTP) delivered via email. We do not store passwords.
- Automatic session timeout or re-authentication controls designed to protect account access.

- Authentication tokens with automatic expiry; refresh tokens are revoked upon logout.

Because sign-in depends on one-time passcodes delivered to your registered email address, you are responsible for maintaining control of that email address. If you lose access to your registered email address, or if it is compromised, the security of your account and your ability to access it may be affected. Notify us promptly if you lose control of your registered contact methods.

No security system is impenetrable. While we use commercially reasonable measures to protect your information, we cannot guarantee absolute security. In the event of a data breach that affects your personal information, we will notify you in accordance with applicable law.

7. Data Retention

We retain your account information and documents for as long as your account remains active. You may delete individual documents at any time through the Application.

When you delete your account, we will delete or de-identify your account data and uploaded documents from active systems within 30 days after account deletion, subject to backup retention, legal obligations, security, fraud prevention, and audit requirements. Data covered by account deletion includes:

- Your account record and all profile information.
- All uploaded documents, including all stored copies.
- All licensure, certification, and professional credential records and notification history.
- All authentication tokens and push notification tokens.

Backup copies may remain in encrypted backups for a limited period after deletion and will be deleted or overwritten according to our normal backup cycle.

Certain technical records, such as server logs and diagnostic records, may be retained for a limited period for operational and security purposes. These records do not contain your personal document data.

We may retain information for a longer period where required by applicable law or to fulfill a legal obligation. Where required by applicable law, we will provide notice regarding retention practices or user rights.

8. Your Rights and Choices

You have the following rights with respect to your personal information:

- Access: you may access and review the information stored in your account at any time through the Application.
- Correction: you may update or correct inaccurate information in your account profile.
- Deletion: you may delete individual documents or delete your entire account at any time through the Application Settings. Upon account deletion, we will delete or de-identify your account data and uploaded documents from active systems within 30 days, subject to the retention exceptions described in Section 7.
- Deactivation: if you wish to temporarily suspend access to your account without deleting your data, please contact us at the address below.
- Portability: you may request a copy of your personal data by contacting us.

To exercise any of these rights or to make a privacy-related inquiry, please contact us at admin@folayhealth.com.

9. Credentialing Data Sources Disclaimer

PhyCentra does not access, retrieve, or use information from any state medical board, the DEA's registration systems, ABMS or its member boards, the National Practitioner Data Bank (NPDB), or any other official licensing or credentialing database. All information processed by PhyCentra is provided directly by you, the user, through voluntary document upload. PhyCentra is not a credentials verification organization and does not operate as a source of primary source verification for any licensing board, hospital, or employer.

10. Children's Privacy

The Application is intended for physicians, physicians in training, and medical school graduates. It is not intended for children under 13 years of age. Account registration requires users to be at least 18 years of age. We do not knowingly collect personal information from children under 13. If we become aware that we have collected personal information from a child under 13, we will delete that information promptly. If you believe a child under 13 has created an account or has otherwise provided us with personal information, please contact us at admin@folayhealth.com.

11. Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, technology, or applicable law. When we make material changes, we will notify you through the Application or by email to your registered address at least 14 days before the changes take effect. Your continued use of the Application after the effective date of the updated Privacy Policy constitutes your acceptance of the changes.

12. Contact Us

If you have any questions, concerns, or requests regarding this Privacy Policy or our data practices, please contact us at:

Folay Healthcare Technologies LLC

Attn: Privacy Officer

admin@folayhealth.com

<https://www.folayhealth.com>