

DATA RETENTION & DELETION 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. Purpose

This Data Retention and Deletion Policy describes how Foly Healthcare Technologies LLC, the operator of PhyCentra ("PhyCentra," "we," "us," or "our"), retains, manages, and deletes personal information and documents collected through the PhyCentra mobile application and web application (the "Application"). It is intended to complement the PhyCentra Privacy Policy and Terms of Service and to provide users with clear information about their rights regarding their data. In the event of a conflict between this policy and the Privacy Policy, the Privacy Policy controls.

2. Scope

This policy applies to all personal information and documents collected from users of the PhyCentra Application across both the mobile application (iOS and Android) and the web application, including account information, professional information, uploaded professional credential documents, OCR-extracted credential data, credential readiness data, share link records, and authentication data.

3. Data Retention Principles

PhyCentra retains personal information only for as long as necessary to provide the service to you and to fulfill the purposes described in our Privacy Policy. Our retention approach is guided by the following principles:

- We do not retain data beyond what is necessary for the stated service purpose.
- We provide you with control over your data, including the ability to delete individual documents and your entire account at any time.
- We do not sell, license, or otherwise transfer retained data to third parties.
- We treat DEA registration numbers, medical license numbers, and other professional registration identifiers as sensitive professional information, with access restricted throughout the data lifecycle.
- We apply appropriate security controls to all retained data throughout its lifecycle.

4. Retention Periods by Data Category

4.1 Account Information and Profile Data

Account registration information (name, email address, phone number) and professional information (medical specialty, state(s) of licensure, and NPI, if provided) are retained for the life of your active account. Upon account deletion, account and profile data is deleted or de-identified from active systems within 30 days, subject to the exceptions in Sections 5 and 7.

4.2 Uploaded Professional Credential Documents

Uploaded documents — including state medical licenses, DEA registration certificates, board certification records, CME certificates, and malpractice insurance documents — are retained in encrypted storage for the life of your active account. You may delete individual documents at any time through the Application; deleted documents are removed from active systems within 30 days. Upon account deletion, all uploaded documents, including all stored copies in active systems, are deleted within 30 days, subject to backup retention as described in Section 4.9.

4.3 OCR-Extracted Credential Data

PhyCentra uses optical character recognition ("OCR") technology, currently provided by Amazon Textract, a service of Amazon Web Services, to automatically read and extract information from documents you upload — such as license numbers, DEA registration details, expiration dates, certification dates, and CME credit hours — without requiring you to type that information manually. Data extracted via OCR is retained for the life of your active account and is deleted with the associated document or upon account deletion.

Documents are transmitted to Amazon Textract solely for the purpose of extraction. Temporary processing copies created during extraction are discarded once processing is complete, and extracted text is returned to PhyCentra's own storage environment. PhyCentra has configured its Amazon Web Services organization to opt out of using customer content for the improvement or development of Amazon machine learning services.

4.4 Credential Readiness Data and Reminders

Credential Readiness Scores, dashboard status indicators, reminder configurations, and notification history are retained for the life of your active account and deleted upon account deletion.

4.5 Share Link Records and Access Logs

If you create secure share links for credential readiness packets through the web application, we retain records of active and revoked share links, and we log packet access events, including the date and time a shared link is opened, for security and audit purposes. Shared credential packets automatically expire 30 days after the share link is created unless revoked earlier by you. Share link records are deleted upon account deletion. Access logs are retained for up to 90 days before permanent deletion.

4.6 Authentication Tokens

JSON Web Tokens (JWT) and refresh tokens issued through Supabase Auth expire automatically per their configured expiry periods. Refresh tokens are revoked upon logout. Expired tokens are soft-deleted (marked inactive in the database) and may be retained for a limited period for security audit purposes before permanent deletion.

4.7 Push Notification Tokens

Retained for the life of your active account and deleted upon account deletion.

4.8 Server-Side Logs and Diagnostic Data

Server-side logs and limited diagnostic, security, and performance information generated during the operation of the Application are retained for up to 90 days for operational, debugging, and security purposes. These records do not contain the content of uploaded documents. After 90 days, they are permanently deleted. Diagnostic information is never used for advertising or third-party profiling.

4.9 Backups

Backup copies of data may remain in encrypted backups maintained by our infrastructure provider for a limited period after deletion from active systems and will be deleted or overwritten according to our normal backup cycle, which does not exceed 30 days. Backups are protected by the same security controls as active data and are not used to restore deleted accounts except where necessary for disaster recovery.

4.10 One-Time Passcodes (OTP)

OTP codes are generated server-side, delivered via email, are time-limited and single-use, and are discarded immediately upon use or expiration. OTP codes are not retained.

4.11 Prohibited Content (Patient Information)

PhyCentra is not intended to store patient medical records, protected health information, or patient-identifiable information. If we identify or are notified that an uploaded document appears to contain such information, we may remove, delete, restrict, or refuse to process it, with or without notice, as described in our Terms of Service and Privacy Policy. Documents removed on this basis are deleted from active systems promptly and are not retained except where required by law.

5. Legally Required Retention

PhyCentra may retain certain information beyond the periods described above where required by applicable law, court order, or valid legal process. Examples may include:

- Records relevant to litigation, regulatory investigation, or legal proceedings in which PhyCentra or Foly Healthcare Technologies LLC is involved.
- Records required by applicable state or federal law for a defined retention period.

Where information is retained beyond the standard retention period for legal reasons, that data will be stored securely, access will be restricted to those with a need to know, and it will be deleted as soon as the legal retention obligation has been fulfilled. Where required by applicable law, we will provide notice regarding retention practices or user rights.

6. Account Deletion

6.1 User-Initiated Account Deletion

You may delete your account at any time through the Application Settings (Settings > Account > Delete Account). Account deletion is permanent and cannot be undone. Before deleting your account, we recommend downloading any credential packets, documents, or information you wish to retain, as deleted information cannot be recovered once the deletion process is complete.

Upon deletion, the following data is deleted or de-identified from active systems within 30 days:

- User account record and all profile information.
- Professional profile information, including specialty, licensure states, and NPI.
- All uploaded professional credential documents and all copies in active storage.
- All OCR-extracted credential data.
- All Credential Readiness Scores, dashboard data, reminder configurations, and notification history.

- All share link records.
- All push notification tokens.
- All authentication and refresh tokens.

Once your account is deleted, you will not be able to recover any documents or data previously stored in the Application. Backup copies are handled as described in Section 4.9. Copies of packets that you previously exported, downloaded, or shared with recipients are outside PhyCentra's control and are not affected by account deletion.

6.2 Account Deactivation

If you wish to temporarily suspend access to your account without deleting your data, you may request account deactivation by contacting PhyCentra at admin@folayhealth.com. A deactivated account retains your data but prevents login access. You may reactivate your account at any time by contacting us. Deactivated accounts that remain inactive for more than 24 months will be subject to permanent deletion in accordance with this policy, following notice to your registered email address.

6.3 Operator-Initiated Deletion

PhyCentra reserves the right to delete accounts that are found to be in violation of the Terms of Service or that are otherwise determined to pose a risk to the Application or other users. Users will be notified prior to deletion where practicable.

7. Data Deletion Requests

In addition to in-app account deletion, you may submit a data deletion request by contacting PhyCentra at admin@folayhealth.com. We will respond to verified deletion requests within 30 days. We may request verification of your identity before processing a deletion request.

Certain information may be exempt from deletion where retention is required by applicable law or where the information is necessary to resolve a dispute or enforce our Terms of Service.

8. User Rights by Jurisdiction

8.1 California Residents

California residents may have additional rights under the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), including the right to know what personal information we collect, the right to delete personal information, the right to correct inaccurate personal information, and the right to opt out of the sale or sharing of personal information. PhyCentra does not sell or share personal information as those terms are defined under California law. To exercise your California privacy rights, contact us at admin@folayhealth.com.

8.2 Other State Privacy Laws

Several states have enacted or are enacting comprehensive consumer privacy laws. As PhyCentra serves users across the United States, we are committed to reviewing and updating this policy as additional state privacy laws take effect. Users in Virginia, Colorado, Connecticut, Texas, and other states with applicable privacy laws may have rights similar to those described above. Contact us at admin@folayhealth.com to exercise any applicable rights.

9. Security During Retention

All data retained by PhyCentra is stored in the United States on infrastructure operated by Supabase, whose platform is hosted on Amazon Web Services, using the following security measures:

- Encryption of documents and personal data at rest and in transit, applied by our infrastructure providers using industry-standard encryption.
- Secure API communications using TLS/HTTPS protocols.
- Access controls restricting data access to authorized personnel only, with heightened restrictions for sensitive professional identifiers such as DEA and license numbers.
- Row-level access controls in the application database limiting each user's data to that user.
- Automatic session expiry and token revocation to limit unauthorized access.

We periodically review and update our security practices to help protect user information as our services evolve and applicable security standards change.

10. Changes to This Policy

We may update this Data Retention and Deletion Policy from time to time. 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.

11. Contact Us

For questions about this policy or to submit a data deletion request:

Folay Healthcare Technologies LLC

Attn: Privacy Officer

admin@folayhealth.com

<https://www.folayhealth.com>