ONYESYNC TERMS OF USE

Last Updated: October 23, 2026

Effective Date: October 12, 2026

1. INTRODUCTION & ACCEPTANCE

OnyeSync is a cloud-based healthcare data platform that enables secure retrieval, storage, and sharing of medical imaging data (DICOM images) and radiology reports across authorized healthcare providers and facilities. OnyeSync is operated by Onye Inc. (“Onye”).

By accessing or using OnyeSync ("the Service"), you agree to be bound by these Terms of Use ("Terms"). If you do not agree to all terms, do not use the Service.

2. DEFINITIONS

Authorized Users: Employees, contractors, or agents of Customer who are authorized by Customer to access OnyeSync and have completed HIPAA training and signed applicable confidentiality agreements.

Business Associate Agreement (BAA): A separate legal agreement required by HIPAA 45 CFR § 164.502(e) and 45 CFR § 164.504(e) governing Onye's handling of Protected Health Information (PHI).

Covered Entity (CE): Healthcare providers, health plans, and healthcare clearinghouses as defined by HIPAA.

Customer: The healthcare organization (hospital, imaging center, clinic, or other Covered Entity) or Business Associate entering into these Terms with Onye for the purpose of using the Service.

De-Identified Data: Data that has been de-identified in compliance with HIPAA Safe Harbor method (45 CFR § 164.514(b)) such that it is no longer Protected Health Information and does not identify any individual.

Protected Health Information (PHI): Any individually identifiable health information including DICOM imaging files, patient demographics, clinical data, and biometric data.

Service or Platform: OnyeSync’s cloud-based software platform for retrieving, displaying, storing, standardizing, sharing, and securely transmitting medical imaging data, radiology reports, and related health information. Where enabled for Customer under the Services Agreement, the Service may include Patient Access API services, retrieval through TEFCA Individual Access Services, FHIR R4 data normalization, patient identity matching, and secure API integrations.

Service Order: A separate written order specifying the particular services to be provided, Service fees, term length, and other commercial terms specific to Customer's engagement with Onye.

3. PERMITTED USES & PROHIBITED CONDUCT

3.1 Permitted Uses

• Retrieve medical imaging and radiology reports from connected PACS systems and other authorized source systems

• Where enabled under the Services Agreement, retrieve patient health information via Patient Access API services and TEFCA Individual Access Services

• Where enabled under the Services Agreement, normalize and standardize data into FHIR R4 format and match patient identities across multiple healthcare providers

• Store and display imaging and reports to Authorized Users for treatment and clinical decision-making

• Share imaging and reports with referral providers designated by Customer, as permitted by HIPAA

- Generate reports, maintain audit trails, and use authorized technical-support functionality
- Transmit PHI to Customer via secure API where enabled under the Services Agreement
- Conduct de-identified analytics in accordance with these Terms and applicable law

All users must comply with HIPAA Privacy Rule, HIPAA Security Rule, HIPAA Breach Notification Rule, State privacy laws (if more restrictive), and Patient informed consent.

3.2 Prohibited Uses

- Sharing PHI without patient authorization or legal basis
- Using PHI for non-treatment purposes (marketing, research without consent)
- Selling or licensing PHI to third parties
- Disclosing PHI to family members without patient consent
- Using credentials of another user
- Sharing login credentials with non-employees
- Downloading imaging for storage outside authorized systems
- Violating any federal, state, or local healthcare law

Violation of any prohibited use will result in: immediate account suspension, termination of these Terms, potential referral to OCR, and liability for damages.

4. USER RESPONSIBILITIES & SECURITY OBLIGATIONS

4.1 Customer Responsibilities

Authentication & Access Control:

- Customer maintains sole responsibility for all Authorized Users
- Customer must verify user identity before granting access
- Customer must revoke access immediately upon employee termination
- Customer must ensure users complete HIPAA training before first use
- Customer must implement multi-factor authentication (MFA) as required

5. DATA OWNERSHIP & CONTROL

You own all PHI. Customers retain ownership of all Protected Health Information uploaded to or accessed through OnyeSync. Onye is a custodian only.

De-Identified Data Ownership Exception: Customer grants Onye the right to de-identify PHI in compliance with the HIPAA Safe Harbor method. Onye owns and retains all De-Identified Data and may use it for analytics, research, benchmarking, and other lawful purposes, subject to applicable law and provided that Onye does not re-identify the data.

6. SERVICE AVAILABILITY & TECHNICAL STANDARDS

6.1 Service Level Agreement (SLA)

Onye targets 99.9% monthly uptime with planned maintenance windows on Sundays 2–4 AM ET.

7. LIABILITY, INDEMNIFICATION & INSURANCE

SUBJECT TO THE LIMITS AND EXCLUSIONS IN THE BAA FOR MATTERS COVERED BY THE BAA, ONYE'S TOTAL AGGREGATE LIABILITY FOR ANY CLAIMS SHALL NOT EXCEED THE FEES PAID BY CUSTOMER IN THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO THE CLAIM.

8. TERM, TERMINATION & DATA DELETION

These Terms continue for the initial Service term specified in the Service Order (typically 1–3 years). Unless either party provides written notice of non-renewal at least 90 days before expiration, these Terms automatically renew for successive one-year periods.

8.1 Data Retention During Active Term

While Customer's account is active, Onye retains all PHI for up to seven (7) years from the date of creation or last access, or as otherwise required by law. Audit logs are retained separately for a minimum of six (6) years as required by HIPAA.

8.2 Data Deletion Upon Termination

Upon termination of these Terms, and subject to the BAA, Onye shall, at Customer's election, return or destroy all PHI from production systems within thirty (30) days of the termination date. All backup copies of PHI shall be destroyed or cryptographically erased within sixty (60) days, and Onye shall provide written certification of return or destruction. Audit logs may be retained for the full six (6) year retention period required by HIPAA. Upon Customer's request made before termination or during the thirty (30) day period, Onye shall make PHI available for export in a standard format (such as DICOM and PDF) before deletion or destruction.

8.3 Notices

All notices under these Terms must be in writing. Notices to Customer will be sent to the email address on Customer's account. Notices to Onye must be sent to info@onyeone.com.

ACKNOWLEDGMENT

By accessing or using OnyeSync, you acknowledge that:

1. You have read and understood these Terms
2. You are authorized to bind your organization to these Terms
3. You have reviewed and agree to the BAA
4. Your organization is a HIPAA Covered Entity or Business Associate
5. You will comply with all HIPAA requirements