

Artificial Intelligence Policy

Last updated March 18, 2026

This Artificial Intelligence Policy describes how Oasys Health, Inc. ("Oasys," "we," "us," or "our") develops, deploys, and governs artificial intelligence features within the Oasys platform.

This policy supplements our Privacy Policy and our agreements with customers, including our Software-as-a-Service Agreement and Business Associate Agreement (BAA) where applicable.

1. Purpose of AI Features

Oasys provides certain products, features, and tools powered by artificial intelligence, machine learning, or similar technologies (collectively, "AI Products").

These AI Products are designed to assist behavioral health providers by supporting workflows such as:

- transcription of therapy sessions
- generation of draft clinical notes
- automated summaries and documentation
- analysis of structured or unstructured data
- AI-generated insights or analytics
- conversational assistance within the platform

AI Products are intended to support clinical workflows and administrative tasks, not to replace the independent judgment of licensed professionals.

2. Human Oversight and Clinical Responsibility

AI-generated outputs (including transcriptions, summaries, draft notes, and analytic insights) may contain errors, omissions, or biases and should not be relied upon without review. Our AI Products are designed to support clinicians, not to make autonomous clinical or eligibility decisions. Clinicians/Providers must review AI-generated content for accuracy and appropriateness, exercise their professional judgment, and are able to override, correct, or disregard any AI-generated outputs. Users should not rely solely on AI-generated outputs for diagnosis, treatment decisions, or other consequential decisions about patients.

3. Use of Protected Health Information (PHI)

When Providers use our AI Products for transcription, note creation, or analytical features, those AI Products may process protected health information ("PHI") on behalf of covered entities. Oasys acts as a Business Associate under HIPAA in providing these Services, and we treat PHI processed by AI Products in accordance with the HIPAA Privacy, Security, and Breach Notification Rules and applicable state health privacy laws. We apply the same administrative, physical, and technical safeguards to PHI in AI workflows as we do to PHI elsewhere in our platform, including access controls, encryption, and audit logging.

4. AI Service Providers and Business Associate Subcontracts

Certain AI Products rely on third-party service providers ("AI Service Providers") to process data and generate outputs requested by users. These AI Service Providers currently include OpenAI, which provides foundation models that power certain transcription, documentation, and conversational features. Where AI Service Providers create, receive, maintain, or transmit PHI on our behalf, we enter into Business Associate Agreements or equivalent agreements that extend HIPAA obligations to those AI Service Providers, including limitations on use and disclosure, implementation of appropriate safeguards, and breach reporting obligations. AI Service Providers may use PHI only to provide the contracted AI functionality to Oasys and our customers, and may not use PHI to train generalized models or for their own independent purposes.

5. Data Use, Training, and De-Identification

Oasys does not use identifiable customer or patient data submitted through the Services to train generalized artificial intelligence models.

This includes identifiable:

- patient data
- clinical notes
- session transcripts
- provider documentation
- other customer-submitted content

However, Oasys may use aggregated or de-identified information to:

- operate and maintain the Services
- improve product performance and reliability
- develop and refine machine learning systems
- enhance platform functionality

When we rely on de-identified data derived from PHI, we implement and periodically review de-identification methods designed to prevent re-identification while maintaining data utility.

6. Minimum Necessary Data Principles

We design our AI Products to comply with HIPAA's minimum necessary standard. Access to PHI within AI workflows is limited to the information reasonably necessary to perform the requested transcription, documentation, or analytic functions, and is further restricted through role-based access controls and technical safeguards. We do not require disclosure of entire medical records to AI Products unless such access is reasonably necessary for the requested use and permitted under applicable law and our agreements with customers.

7. Security and Privacy Safeguards

AI systems are incorporated into Oasys' broader security and privacy program, which includes policies and safeguards designed to protect sensitive information.

While no system can guarantee absolute security, Oasys takes reasonable steps to protect data processed through AI Products from:

- unauthorized access
- misuse
- accidental disclosure
- security threats

8. Fairness, Nondiscrimination, and Risk Management

Oasys evaluates its AI Products for potential risks, including the risk of unfair or discriminatory impacts, particularly where outputs may influence clinical documentation, care pathways, or access to services. We incorporate AI-related risks into our security and privacy risk analysis and take reasonable measures to monitor, test, and update AI functionalities to mitigate identified risks, consistent with guidance from the U.S. Department of Health and Human Services and other regulators. Our policies and training emphasize that AI tools must not be used in ways that result in unlawful discrimination on the basis of race, color, national origin, sex, disability, or other protected characteristics.

9. Patient Access and Transparency

When AI-generated notes, summaries, or insights are made available to patients through the Oasys platform, such content will be clearly associated with the provider's account, and providers are responsible for determining what information is appropriate to share. Where required by law, we and our covered-entity customers will inform patients when AI-enabled tools are used in generating documentation or insights that may influence their care or records, and will provide legally required avenues to request clarification or human review of such outputs.

10. State Law and Additional Rights

Residents of certain U.S. states may have additional rights under privacy or AI-specific laws related to automated or AI-assisted processing of their personal information, including rights to receive more information about how AI is used, to request human review of certain AI-influenced decisions, or to limit certain types of profiling. Where such laws apply, Oasys will honor those rights in coordination with our covered-entity customers, as described in the "United States Residents' Privacy Rights" section of this Privacy Notice.

11. Updates to This Policy

Oasys may update this AI Policy from time to time to reflect:

- changes in our AI technologies
- regulatory developments
- improvements to our governance practices

Updated versions will be posted on our website with a revised effective date.

12. Contact Information

If you have questions about this policy or Oasys' use of artificial intelligence, please contact:

Oasys Health, Inc.

Email: privacy@oasys.health

Website: <https://oasys.health>