

Whadata Health Data Privacy Policy

Date of Policy: December 6, 2024

Whadata AI, Inc. (“Whadata,” “we,” “us,” or “our”) recognizes the sensitive and confidential nature of Protected Health Information (“PHI”) and is committed to safeguarding it in accordance with the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), the Health Information Technology for Economic and Clinical Health Act (“HITECH”), and all applicable privacy and security regulations (collectively “HIPAA Rules”). This Health Data Privacy Policy (“Policy”) explains how we handle PHI wh...

This Policy applies solely to PHI that Whadata receives, maintains, or transmits on your behalf in connection with the Services. For information on how we handle non-PHI personal information, please refer to our General Privacy and Cookies Policy.

1. Purpose and Scope

This Policy describes how Whadata protects and uses PHI in compliance with HIPAA Rules. When we act as a Business Associate to a Covered Entity, we agree to comply with the terms of the Business Associate Agreement (“BAA”) executed with that Covered Entity. The BAA, together with this Policy, governs our privacy and security obligations regarding PHI.

2. Definitions

- **Protected Health Information (PHI):** PHI includes any individually identifiable health information relating to an individual’s health condition, provision of healthcare, or payment for healthcare that Whadata creates, receives, maintains, or transmits on behalf of a Covered Entity.
- **Covered Entity:** A healthcare provider, health plan, or healthcare clearinghouse subject to HIPAA.
- **Business Associate:** A person or organization, other than a workforce member of a Covered Entity, that performs activities or services involving the use or disclosure of PHI on behalf of a Covered Entity.

3. Our Role Under HIPAA

Whadata typically serves as a Business Associate to Covered Entities using our Services. As such, we may create, receive, maintain, or transmit PHI on behalf of Covered Entities as permitted by the HIPAA Rules and the BAA. We will not use or disclose PHI except as allowed under the BAA, this Policy, HIPAA Rules, or as required by law.

3.1 Enterprise Clients and Role of Covered Entity

Where the Services are used by an enterprise client (e.g., healthcare group, clinic, or provider network), the Covered Entity is solely responsible for:

- Designating authorized users and managing user permissions;
- Responding to access, amendment, or disclosure log requests from individuals;
- Ensuring compliance with internal privacy and security policies.

Whadata, acting as Business Associate, supports enterprise clients by providing administrative controls, audit logs, and user activity tracking features, but does not assume responsibility for how PHI is accessed or used internally by the Covered Entity's personnel.

4. How We Use and Disclose PHI

- **Permitted Uses and Disclosures:** We may use or disclose PHI as necessary to provide the Services, for example, to process patient data, facilitate treatment-related communications among authorized healthcare professionals, support payment activities (if contracted), or assist in healthcare operations as defined by HIPAA, such as quality improvement or analytics.
- **Minimum Necessary:** We will make reasonable efforts to ensure that access to and disclosure of PHI is limited to the minimum amount necessary to accomplish the intended purpose, in accordance with HIPAA's "minimum necessary" standard.
- **Authorizations:** We will not use or disclose PHI for purposes outside the scope of treatment, payment, or healthcare operations without a valid, written patient authorization or as otherwise permitted or required by the HIPAA Rules.

5. Individual Rights

While Covered Entities are responsible for managing patient requests related to PHI, our Services are designed to support compliance with individual rights under HIPAA, including:

- **Right of Access:** Covered Entities may use our Services to retrieve and provide patients with their PHI.
- **Right to Amend:** We can support Covered Entities in amending PHI within our system as directed, maintaining audit trails of changes.
- **Right to Accounting of Disclosures:** Our Services maintain logs of certain disclosures to help Covered Entities comply with accounting requirements.

5.1 Support for HIPAA Rights

Whadata's platform is designed to support the Covered Entity's obligations under HIPAA regarding:

- Individual access to PHI;
- Requests for amendment;
- Accounting of disclosures.

Covered Entities remain responsible for managing and responding to such requests. Upon request, Whadata will assist in providing the necessary data, logs, or audit records in a timely manner.

6. Administrative, Physical, and Technical Safeguards

We implement appropriate administrative, physical, and technical safeguards to protect PHI:

- **Administrative Safeguards:** We conduct regular risk analyses, implement policies and procedures for workforce training and sanctions, and maintain contingency plans for emergencies.
- **Physical Safeguards:** We secure servers and restrict physical access to facilities storing PHI, using measures like controlled access, locked server rooms, and proper device disposal protocols.
- **Technical Safeguards:** We use access controls, encryption (in transit and at rest), unique user identification, audit logs, and integrity checks to protect PHI from unauthorized access, alteration, or disclosure.

6.1 Subprocessor Security and Transparency

Whadata engages trusted third-party service providers (e.g., hosting, cloud infrastructure, analytics, and communications) that are contractually bound to safeguard PHI and comply with HIPAA. All subprocessors are vetted for technical and organizational security measures. A list of key subprocessors is available upon request.

7. Business Associate Agreements (BAAs)

We enter into BAAs with all Covered Entities or upstream Business Associates. Each BAA outlines the permitted uses and disclosures of PHI, our obligations regarding security and breach notification, and our commitment to comply with HIPAA Rules. In the event of any conflict between this Policy and the BAA, the BAA will govern with respect to PHI.

8. Breach Notification

In the event of a breach of unsecured PHI, we will provide the required notifications to the Covered Entity in accordance with HIPAA's Breach Notification Rule and our BAA. We will cooperate with the Covered Entity in investigating and mitigating the breach and, if requested, assist in providing the required notifications to affected individuals and regulators.

9. Data Retention and Destruction

We will retain PHI as required to fulfill the purposes outlined in our agreement with you or as required by law. When PHI is no longer needed, we will securely destroy or return it in accordance with the BAA and HIPAA standards, employing methods that render the PHI unusable, unreadable, or indecipherable.

10. International Transfers and Localization

Whadata may process PHI in the United States or other jurisdictions where its infrastructure or subprocessors operate. If required by law or requested in writing by a Covered Entity, Whadata will:

- Evaluate the feasibility of regional or in-country hosting options;

- Implement appropriate safeguards, such as Business Associate Agreements, access restrictions, encryption, and contractual commitments to meet data residency or localization obligations;
- Avoid transferring PHI across borders unless required by the Services and permitted by applicable HIPAA rules and other laws.

By using the Services, Covered Entities acknowledge and agree to these data transfer mechanisms unless otherwise negotiated.

11. Complaints and Concerns

If you have concerns about our handling of PHI, please contact us at:

Email: support@whadata.com

Patients may direct any requests or complaints to their Covered Entity. We will promptly assist the Covered Entity, as appropriate, in addressing such concerns.

12. Changes to This Policy

We may update this Policy as necessary to ensure continued compliance with HIPAA or to reflect changes in our Services. We will notify Covered Entities of significant updates. The latest version of this Policy will be made available to Covered Entities.

13. Governing Law

This Policy is governed by and shall be interpreted in accordance with applicable federal and state laws, including HIPAA and its implementing regulations.