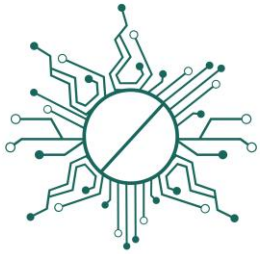


Pharmlytix™ HIPAA Privacy & Security Notice

Effective Date: October 14th 2025

Pharmlytix™ ("we," "our," or "us") is committed to maintaining the privacy and security of Protected Health Information ("PHI") as required under the **Health Insurance Portability and Accountability Act of 1996 (HIPAA)** and the **Health Information Technology for Economic and Clinical Health Act (HITECH)**.

This **HIPAA Privacy & Security Notice** describes how PHI may be used and disclosed within the secure Pharmlytix™ application (**app.pharmlytix.ai**), how we protect that information, and your rights regarding PHI under federal law.

1. Scope

This Notice applies only to users of app.pharmlytix.ai— the secure, clinical decision support platform used by consultant pharmacists, facilities, and healthcare providers.

If you are visiting our **public website (www.pharmlytix.ai)**, please review the separate **Public Website Privacy Policy** that governs informational and marketing data.

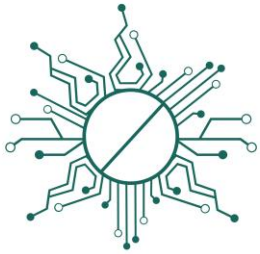
2. Our Role Under HIPAA

Pharmlytix™ acts as a **Business Associate (BA)** to our clients, who may be covered entities (e.g., skilled nursing facilities, assisted living facilities, consultant pharmacies, or healthcare providers).

Under Business Associate Agreements (BAAs), we handle PHI on behalf of these entities for the purpose of providing medication management and clinical decision support services.

Pharmlytix™ does not own or control PHI; it remains the property of the covered entity.

3. Protected Health Information (PHI)



“Protected Health Information” refers to any individually identifiable health information transmitted or maintained in electronic or other form, including but not limited to:

- Resident or patient names, medical record numbers, or facility identifiers
- Diagnoses, medications, and treatment information
- Dates of admission, discharge, or birth
- Any other data that can reasonably identify an individual in connection with healthcare services

4. How Pharmlytix™ Uses and Discloses PHI

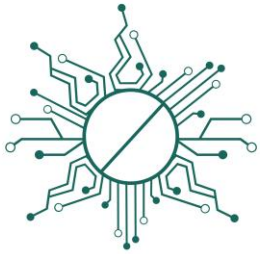
Pharmlytix™ uses and discloses PHI only as permitted under HIPAA, HITECH, and our BAAs, and **only to support the healthcare operations** of our clients.
Typical uses include:

A. Permitted Uses

- **Clinical Decision Support:** Generating AI-assisted medication management recommendations, drug interaction checks, and therapeutic guidance for licensed pharmacists and providers.
- **Quality Assurance:** Monitoring platform performance, improving accuracy, and preventing model drift or bias.
- **Customer Support & Troubleshooting:** Accessing limited PHI only when necessary to resolve technical or data-related issues, under strict access controls.
- **Data Integrity & Security Monitoring:** Ensuring ongoing accuracy, validity, and safe operation of PHI within the system.

B. Permitted Disclosures

- **To Authorized Users:** Licensed professionals or organizations with verified access rights under the covered entity’s authorization.



- **To Subcontractors:** Only to HIPAA-compliant subcontractors (e.g., cloud hosting or AI infrastructure partners) under signed Business Associate Agreements.
- **For Legal Compliance:** As required by law, regulation, subpoena, or government oversight, after appropriate review and documentation.
- **For System Maintenance or Threat Prevention:** When necessary to protect the confidentiality, integrity, and availability of PHI.

Pharmlytix™ **never** uses PHI for marketing, advertising, or AI model training without explicit written authorization.

5. Prohibited Uses

Pharmlytix™ and its subcontractors are expressly prohibited from:

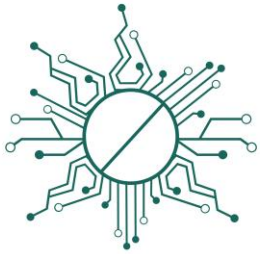
- Selling or renting PHI for any purpose
- Using PHI for marketing or commercial gain
- Combining PHI with external datasets to build unrelated AI models
- Accessing PHI for any reason outside the scope of contracted services

6. Data Security and Safeguards

Pharmlytix™ maintains a robust, multi-layered security framework that complies with **HIPAA Security Rule (45 CFR §§ 164.302–318)** standards.

Administrative Safeguards

- Business Associate Agreements with all covered entities and subcontractors
- Security and privacy awareness training for all personnel
- Role-based access controls and least-privilege enforcement
- Risk analyses, mitigation plans, and regular security audits



- Incident response and breach notification procedures

Technical Safeguards

- Encryption of PHI **in transit (TLS 1.2+)** and **at rest (AES-256)**
- Multi-factor authentication (MFA) for all administrative access
- Continuous logging and audit trails of PHI access and modifications
- Segregated production environments with role-based API access
- Ongoing vulnerability scanning and patch management

Physical Safeguards

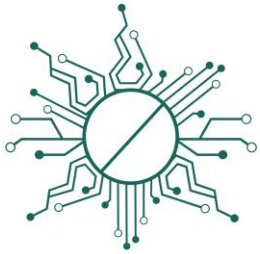
- PHI hosted in secure, SOC 2 Type II–certified data centers
- Redundant backups and disaster recovery protocols
- Strict access controls to physical hardware and servers

7. Model Transparency and AI Governance

Pharmlytix's™ AI-driven decision support functions operate under a framework aligned with the **ASCP FAVES principles** — ensuring all algorithms are **Fair, Appropriate, Valid, Effective, and Safe**.

We maintain:

- Transparent, explainable AI logic referencing recognized clinical standards (e.g., Beers Criteria, renal dosing, CMS guidance).
- Regular bias and drift audits, especially for older adult populations.
- Versioned models with documented validation and audit history.
- A formal **AI Ethics & Validation Committee** overseeing algorithm updates and compliance with ONC's HTI-1 transparency requirements.



8. User Responsibilities

Authorized users of Pharmlytix™ agree to:

- Access PHI only as necessary for their professional role.
- Maintain secure credentials and log out when sessions end.
- Avoid downloading, exporting, or redistributing PHI outside approved workflows.
- Report any suspected unauthorized access, misuse, or security concernsĂ immediately to **security@pharmlytix. ai**.

9. Data Retention and Destruction

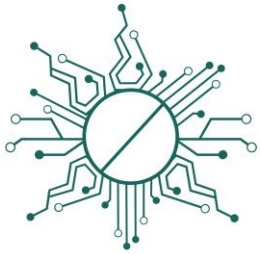
PHI is retained only for as long as necessary to fulfill service obligations or as required by the covered entity.
Upon termination of a client contract or at the client's request, Pharmlytix™ securely deletes or returns PHI using industry-standard sanitization protocols (NIST 800-88).

10. Breach Notification

In the event of a data breach involving PHI, Pharmlytix™ will:

- Investigate promptly and mitigate the impact.
- Notify affected covered entities **without unreasonable delay** and no later than **60 days** after discovery.
- Cooperate with client entities in their notification duties to affected individuals and regulators as required by law.

11. Individual Rights



Individuals whose PHI is maintained by Pharmlytix™ through a covered entity have rights under HIPAA, including:

- The right to access or request copies of their PHI (through the covered entity).
- The right to request amendments or corrections.
- The right to an accounting of certain disclosures.
- The right to file a complaint regarding privacy practices.

Requests related to these rights should be directed to the covered entity (e.g., the facility or pharmacy), which will coordinate with Pharmlytix™ as necessary.

12. Changes to This Notice

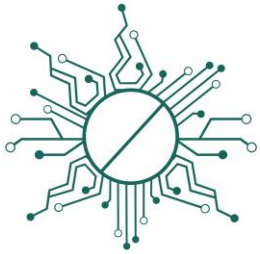
Pharmlytix™ may update this HIPAA Privacy & Security Notice periodically to reflect changes in our services, practices, or applicable law.
Revisions will be posted within the secure platform and communicated to clients as appropriate.
The revised effective date will be listed at the top of this document.

13. Contact Information

For privacy, security, or compliance inquiries, please contact:

Pharmlytix™ Privacy & Security Officer
Email: **security@pharmlytix.ai**
Mailing Address: 4351 W Tischer Rd, Duluth, MN 55803
Website: https://app.pharmlytix.ai

If you believe your privacy rights have been violated, you may also file a complaint directly with the **U.S. Department of Health and Human Services Office for Civil Rights (OCR)** at:
https://www.hhs.gov/ocr/privacy/hipaa/complaints/



Pharmlytix™ will not retaliate against any individual or entity for filing a complaint in good faith.