daw

PRIVACY POLICY FOR APPLICATION AND SERVICE USERS

Effective Date: June 12, 2025

PRIVACY POLICY FOR APPLICATION AND SERVICE USERS
View any updates to the policy here: https://dawsystems.com/pdf/privacypolicy

Your privacy is important to us. This Privacy Policy ("Policy") describes how D.A.W. Systems, Inc. ("DAW") collects, stores, processes, and secures PHI and your personal user information through its Services and how such information is used.

Scope and Incorporation: This Policy applies to DAW websites, applications, platforms, communication tools, integrations, and related offerings that share or communicate your data and devices ("Services"). By using our Services, you acknowledge and accept this Policy, which is incorporated by reference into the DAW Terms of Use ("EULA"). Use of our Services is governed by U.S. law and is intended only for users in the United States who are 18 years of age or older. Approved healthcare providers, guardians, or parents may use the Services on behalf of minors, but under no circumstances may the Services be used directly by individuals under age 18. The Terms of Use may further define or restrict privacy-related rights or duties; in the event of a conflict, the Terms of Use shall control.

HIPAA and FERPA Applicability: Provisions in this Policy referring to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") apply only if HIPAA is applicable to you or your organization. If your organization is instead subject to the Family Educational Rights and Privacy Act ("FERPA"), those rules shall control and supersede HIPAA-related obligations. It is the sole responsibility of each user, account holder, or business to determine whether HIPAA or FERPA applies. DAW is not liable for incorrect determinations regarding their applicability. *Example: A school-based clinic may be governed by FERPA instead of HIPAA when operating under an educational institution.*

1. Information Reported or Submitted Using Our Services: You may provide information by:

- Direct data entry during sign-up, registration, messaging, or form completion;
- Authorization for us to import data from other users or third-party systems;
- Other user-initiated methods where it is clear you are submitting data to the Services.

2. Use of Information:

a. General Use DAW collects data to operate effectively and personalize user experiences. Data may be collected directly from you, passively through cookies or logs, or via third-party partners (e.g., EMRs used by healthcare providers).

b. Personally Identifiable User Data: Used to:

- Provide, operate, maintain, and improve Services;
- Communicate administrative updates;
- Protect data and respond to legal demands;
- Fulfill other goals outlined in this Policy or Terms of Use.

c. Non-Identifiable Data: Used for:

- Analytics, research, usage trends, audits;
- Developing new features or Services;

- Contextual, non-personalized content delivery;
- Medical and public health research;
- Demographic reporting (e.g., age, geography) without individual identifiers;
- Community features, with user-controlled visibility;
- Compliant sharing with authorized partners (e.g., EMR integrations), including Protected Health Information (PHI) under HIPAA guidelines;
- Communication of product or security updates;
- Aggregated, de-identified disclosures under 45 C.F.R. § 164.514.

d. Use of Patient Identifiable Information for Integrated Services: To facilitate services including but not limited to, eligibility (insurance) identification, real-time benefit checks, and electronic prior authorization (ePA), DAW may transmit identifiable patient information—including name, date of birth, insurance details, and prescription data—to authorized third-party networks and pharmacy benefit processors. These disclosures are made solely to enable the requested transaction or service on behalf of the prescribing provider and their staff and are governed by applicable HIPAA Business Associate Agreements (BAAs). DAW does not authorize reuse or retention of such data by these third-parties beyond what is contractually necessary to complete the transaction. Third-party systems can be used for other Services that allow you to electronically contact your patients; for these Services you must opt-in and your patients must opt-in to receiving these types of communication.

e. Use of De-Identified Data for Platform Optimization and Analytics: DAW may use aggregated or de-identified usage data to train, validate, or enhance platform performance through analytics tools and artificial intelligence systems, including but not limited to service quality benchmarking, bug/error detection, and workflow optimization. This data is not linked to individual user identities or used to target advertising.

(i) Use of De-Identified Data for Machine Learning and Artificial Intelligence

DAW may use aggregated or de-identified usage data to develop, train, and validate machine learning (ML) and artificial intelligence (AI) models that support platform optimization, diagnostics, recommendation systems, clinical workflow enhancements, and operational efficiency. All data used in connection with AI/ML training is de-identified in accordance with HIPAA de-identification standards (45 C.F.R. § 164.514) and is not linked to any individual provider, patient, or end user.

- **Scope**: This includes de-identified prescribing behavior, system interaction logs, session metadata, product utilization patterns, and platform performance signals.
- **Purpose**: Such data may be used to improve decision support, automate quality benchmarking, identify system bottlenecks, or offer enhanced personalized experiences within the Services.
- **Limitations**: DAW does not use patient-identifiable data or Personal Information for AI/ML training purposes unless explicitly authorized in writing or required by law. De-identified data used for AI/ML is not sold or shared in any form that allows re-identification.
- **Third-Party Tools**: Any third-party vendors assisting in AI/ML development must operate under contractual terms requiring strict data protection, use limitations, and prohibitions on re-identification.
- **Transparency**: You may contact DAW at any time to request more information regarding our AI/ML usage or to inquire about opt-out options where applicable under state law.

f. Use of De-Identified Patient Data for Services, Analytics, and External Insights: DAW may use aggregated or de-identified data, consistent with the definitions in our Terms of Use, to support product development, quality benchmarking, and platform performance analytics. All such use is governed by our Terms of Use and complies with HIPAA de-identification standards (45 C.F.R. § 164.514). DAW may derive commercial benefit from such data. We may share de-identified datasets through analytics partnerships, health insights generation, performance reporting, and service optimization under contract for the purposes described above.

See EULA Section 2.6 for complete usage rights.

3. Other Information Captured: DAW captures technical metadata (e.g., device, browser, OS, timestamps, interactions) to troubleshoot and improve Service delivery.
4. Cookies & Tracking: See our Cookie Policy for full details.
5. Vendor Partners: DAW collaborates with certified vendor partners for workflow optimization and data interoperability. Vendor use is governed by their own privacy policies in addition to this Policy.
6. Consents & Authorizations & Third-Party Suppliers: Use of Services constitutes consent to the Terms of Use, this Policy, and any just-in-time consents required by law. We may share limited personal information—such as your name, National Provider Identifier (NPI), medical license number, DEA registration, practice affiliation, and other professional credentials—with trusted third-party suppliers, contractors, or integration partners for operational purposes. This may include identity verification, credentialing, regulatory compliance (e.g., EPCS, PMP), secure routing of prescriptions, and enabling access to applicable platform features. Such third-parties operate under contractual obligations that require appropriate safeguards for your data and prohibit any use beyond the scope of services provided to DAW. We do not authorize these third-parties to use your professional information for marketing or advertising purposes without your express consent.
7. Sharing & Direct Communications: User activities like appointment requests, journal entries, or health sharing include inherent personal user data. Community posts are public **do not post sensitive information**. DAW is not responsible for reposting or indexing of community content.
8. Fees & Payments: For those users of the Services that license DAW Services directly and pay for licenses to DAW, DAW may process payments directly or through third-party vendor partners. Those vendors' privacy and payment terms apply. DAW does not store your credit card or financial data. However, DAW may facilitate the secure transmission of payment information to processors as needed to support the Services. Refunds are discretionary unless required by law. Requests must be submitted within 90 days.
9. Protected Health Information: When acting as a HIPAA Business Associate, DAW complies fully with applicable privacy and security requirements under HIPAA and HITECH.
10. Sharing of User Information: DAW does **not share personally identifiable user data** except:

- When voluntarily shared by users;
- With consent or appropriate legal basis;
- With account administrators;
- With service providers under confidentiality;
- In legal compliance;
- In mergers, sales, or acquisitions;
- For legitimate Services operation as outlined herein.

11. Fraud, Hacking & Illegal Use: DAW monitors use for security risks and may preserve or disclose data in response to abuse, fraud, subpoenas, or threats to integrity. Retention may continue beyond account closure if necessary.
12. Security, Breaches & Notifications: DAW uses best-in-class security practices (e.g., encryption, intrusion detection, patching, user controls). Any breach affecting your data will trigger timely notifications under HIPAA and applicable laws.

13. Contextual Messaging: Use of Professional and Licensing Information for Brand-Awareness and Internal Promotional Content DAW may use your **National Provider Identifier (NPI), practice affiliation, state license information,** and similar publicly available or submitted professional identifiers to deliver **contextual brand-awareness and promotional content** related to the Services. These communications may include:

- Notifications about DAW feature enhancements;
- Professionally relevant opportunities, tools, or product suggestions;
- Educational materials or service updates from DAW or its platform partners. Such content is:
- Shown **only within DAW-controlled interfaces;**
- Based on your specialty, practice geography, or service usage;
- **Not shared externally** with third-party advertisers without your opt-in;
- **Never used for retargeted or external behavioral advertising.** You may opt out of receiving such content at any time via account preferences or by contacting DAW at support@dawsystems.com.

14. Sponsored Messaging and Performance Metrics: Some DAW Services include delivery of sponsored messaging, such as brand awareness content, educational messages, and patient affordability materials (e.g., Co-Pay Coupons). These may appear in clinical workflows or application modules. DAW may derive commercial benefit from these messages based on engagement metrics such as impressions, reach, or frequency, in accordance with our commercial agreements. Interaction data may be collected solely to verify delivery and calculate aggregate metrics. DAW does not share user-level data with third-parties without explicit consent.

15. Authorized Programmatic Access: DAW may grant integration partners limited rights to access, index, or cache portions of its digital properties or application environments for the purpose of delivering sponsored messaging or other embedded services. This access is secured via contract and only used in connection with approved functionality.

16. California and State Privacy Rights: Depending on your jurisdiction (e.g., California, Colorado, Virginia, Connecticut), you may have additional rights regarding your personal user data and PHI data. These may include the right to access, delete, correct, or limit the use of your information, as well as the right to opt-out of the sharing of personal user data for targeted advertising. DAW does not "sell" personal user information as defined under applicable laws. You may exercise these rights by contacting support@dawsystems.com or visiting your user settings.

17. Data Retention: DAW retains data in the applications, including PHI, for as long as necessary to fulfill the purposes outlined in this Policy, to deliver the DAW Services, comply with our legal obligations, resolve disputes, and enforce our agreements.

18. Children's Privacy: DAW Services are not directed to children under the age of 13 and we do not knowingly collect personal information from them. If we discover that a child under 13 has submitted personal data, we will delete it in accordance with the Children's Online Privacy Protection Act (COPPA).

19. Support and Patient Data: Users must not include PHI in support requests, emails, screenshots, or attached files. DAW reserves the right to block or purge any such content upon detection. It is your responsibility to redact sensitive information or use anonymized data when submitting cases. If PHI is submitted inadvertently, DAW will treat such data in accordance with its HIPAA-compliant safeguards and any applicable Business Associate Agreement (BAA). By using the Services and requesting support, you consent to such access and escalation actions, which are performed solely to deliver operational support, maintain compliance, and ensure service continuity.

19. Updates to this Policy: We reserve the right to modify or update this Privacy Policy at any time to reflect changes in law, operational practices, or enhancements to our Services. The most current version of the Policy will be posted on our application website and will indicate the date it was last updated. Where required by law or where the changes materially affect your rights, we will notify you through direct communication or prominent notice within the Services prior to the effective date. Updates

become effective immediately for all new users upon posting. For existing users, updates will become binding fourteen (14) days after notice is provided. Your continued use of the Services following that period constitutes your agreement to the revised Policy. If you do not agree to any updates, you must cease use of the Services and request account deactivation before the effective date applicable to you.

20. Account Termination: To terminate/cancel your account, contact:

D.A.W. Systems, Inc.
Attn: Privacy & Compliance
585 Troy-Schenectady Road, Suite 2
Latham, NY 12110
support@dawsystems.com

21. Governing Law and Forum Selection: This Policy is governed by and interpreted in accordance with the laws of the United States and the State of New York, without regard to conflict of law principles. The exclusive forum for any dispute arising out of or relating to this Privacy Policy shall be the state or federal courts located in Albany County, New York. You consent to the jurisdiction and venue of such courts and waive any objection to their convenience or propriety.