

ONA HEALTH SOLUTIONS INC.

PLATFORM PRIVACY POLICY

Latest version date: 7th July 2026

1. WHAT THIS POLICY COVERS

Ona Health Solutions Inc. (“**Ona**”, “we”, “us”) provides an all-in-one practice management platform to healthcare practices in the United States. This policy explains how we handle personal information when we act **on our own behalf** — that is, as the controller of that information.

It covers:

- **Practices and their personnel** who subscribe to, administer or use the Platform.
- **Prospective customers** who request a demo, contact us or interact with our sales team.
- **Visitors** to ona.health and our other public web pages.

This policy applies to personal information we collect through the Platform, our websites, and our email, telephone and messaging communications.

2. WHAT THIS POLICY DOES NOT COVER — PATIENT HEALTH INFORMATION

This policy does not govern patient health information.

When a healthcare practice uses the Platform to deliver care, that practice is a **covered entity** under the Health Insurance Portability and Accountability Act (“HIPAA”) and Ona is its **business associate**. Patient information in the Platform — including chart notes, transcripts, prescriptions, orders, consents, claims, messages and patient portal content — is **Protected Health Information (“PHI”)**.

Our handling of PHI is governed exclusively by:

- HIPAA and its implementing rules at 45 CFR Parts 160 and 164; and
- the **Business Associate Agreement** in place between Ona and the practice.

We process PHI only as that agreement permits, and only on the practice’s instructions. **We are not the controller of PHI and this policy grants no rights in respect of it.**

If you are a **patient**, the organisation responsible for your health information is **the practice that treats you**, not Ona. Requests to see, correct, restrict or obtain an accounting of your health records must go to your practice, which will provide its own Notice of Privacy Practices

describing your rights. If you contact us directly about your health records, we will refer you to your practice.

3. THE THREE RELATIONSHIPS, IN SHORT

Whose information	Who is responsible	Governed by
Patient health information in the Platform	The practice (covered entity); Ona acts as business associate	HIPAA and the Business Associate Agreement
Practice, administrator and staff account information	Ona, as controller	This policy
Website visitors and prospective customers	Ona, as controller	This policy

4. INFORMATION WE COLLECT

4.1 Practice and account information

Practice or legal entity name, business address, tax identification number, National Provider Identifier and taxonomy, state licence and DEA registration details where required for a feature, specialty, locations, and the identity of authorised signatories and administrators.

4.2 Authorized User information

Name, business email address, business telephone number, job title, role and permissions, professional credentials and licence details, authentication data (hashed passwords, multi-factor authentication settings, session tokens), and preferences.

4.3 Billing information

Billing contact details, subscription and seat history, invoices, transaction records and payment status. **Card and bank details are collected and stored by our payment processor, not by Ona.** We receive only limited identifiers such as card type, last four digits and expiry.

4.4 Usage, device and log data

IP address, browser and device type, operating system, approximate location derived from IP address, pages and features accessed, actions taken, timestamps, referring page, crash and error reports, and audit log entries recording who accessed what within the Platform.

4.5 Support and communications

The content of support tickets, in-app chat, emails and calls with our team, including any attachments or screenshots you send us. **Please do not include patient information in support requests unless it is necessary; where you do, it is handled as PHI under the Business Associate Agreement.**

4.6 Website visitors and prospective customers

Information you submit through demo request, contact and newsletter forms — typically name, business email, practice name, specialty, size and message. Plus cookie and analytics data as described in Section 9.

4.7 Information we do not want

We do not seek, and ask you not to send us, your own sensitive personal information — such as government identifiers, financial account numbers, or your personal health information — except where a specific feature requires it and says so.

5. HOW WE USE INFORMATION

We use the information described above to:

- provide, operate, maintain and secure the Platform;
 - create and administer accounts, seats and permissions;
 - authenticate users and prevent unauthorised access;
 - process subscriptions, calculate usage-based charges and collect payment;
 - provide support, respond to enquiries and communicate about service issues, maintenance and changes;
 - monitor performance, diagnose faults and improve reliability;
 - develop, test and improve the Platform and its features, subject to Section 7;
 - produce internal analytics and reporting on how the Platform is used;
 - detect, investigate and prevent fraud, abuse, security incidents and violations of our Terms;
 - market and sell the Platform to practices, subject to your choices in Section 10; and
 - comply with law and enforce our agreements.
-

6. LEGAL AND CONTRACTUAL BASIS

We process this information because it is necessary to perform our contract with the practice, because we have a legitimate business interest in operating and improving a secure platform, because you have consented (where we ask for consent), or because the law requires it.

7. ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

This section describes how information is used in connection with the Platform's AI features, including the ambient scribe, automated charting, AI intake and the AI receptionist.

7.1 Patient information. Use of PHI in AI features is governed by the Business Associate Agreement and our Terms of Service, not by this policy. In summary, and as those documents provide: we process PHI to deliver the AI features to the practice; every AI output is a draft

requiring clinician review and signature before it enters the record; and our model providers are contractually prohibited from using PHI to train their own models.

7.2 De-identified data. We may de-identify PHI using the safe harbour or expert determination methods at 45 CFR 164.514(b). Once de-identified, data is no longer PHI. We may use de-identified and aggregated data to operate, evaluate, secure and improve the Platform, including to train, fine-tune, test and evaluate the models used in our AI features, and to produce aggregate statistics and benchmarks.

7.3 We do not sell it and we do not share it. We do not sell, rent, license, trade, monetise or publish de-identified or aggregated data derived from customer data, and we do not disclose it to data brokers, advertisers, pharmaceutical or device companies, payers, insurers, employers or research organisations for their own purposes — whether for payment or free of charge. We will not re-identify de-identified data or attempt to do so. This commitment survives termination and binds our successors, including on any merger, acquisition or change of control.

7.4 Opting out. A practice may opt out of the use of its de-identified data for model training by writing to legal@ona.health. We will give effect to the opt-out prospectively within thirty (30) days. Data already incorporated into a trained model cannot be extracted from it.

7.5 Practice and usage information. We may use account and usage information — as distinct from patient information — to improve the Platform, including to develop and evaluate models that support workflow, scheduling and support features.

8. HOW WE SHARE INFORMATION

8.1 Service providers. We share information with vendors who process it on our behalf, under written contracts restricting their use of it, and under business associate agreements where they handle PHI. They fall into these categories:

Category	Purpose
Cloud hosting and infrastructure	Hosting the Platform and storing data in the United States
E-prescribing	Transmitting prescriptions, including controlled substances
Payment processing	Collecting subscription fees and processing patient payments
Clearinghouse and eligibility	Submitting claims and checking coverage
Telephony, SMS and email	Voice calls, messaging and transactional email
Video infrastructure	Telehealth visits
Laboratory networks	Lab orders and results
AI model providers	Powering AI features, under terms prohibiting training on customer data

Analytics and error monitoring	Understanding performance and diagnosing faults
Customer support and CRM tooling	Managing support requests and sales enquiries

A current list of subprocessors that handle PHI is available on request from legal@ona.health.

8.2 We do not sell personal information. We do not sell personal information, and we do not share it for cross-context behavioural advertising, **except** for the limited marketing-site advertising cookies described in Section 9, which you can opt out of.

8.3 At your direction. We share information with third parties you choose to connect to your workspace. Once information reaches a third party at your direction, that party's own terms and privacy policy apply.

8.4 Legal and safety. We may disclose information where required by law, subpoena, court order or regulator, or where necessary to investigate fraud or protect the rights, safety or property of Ona, our customers or the public. Where we are legally permitted, we will notify the affected practice first.

8.5 Business transfers. If Ona is involved in a merger, acquisition, financing, reorganisation or sale of assets, information may be transferred as part of that transaction. **The commitments in Section 7.3 continue to apply to any successor.** We will give notice before your information becomes subject to a materially different privacy policy.

8.6 Aggregate information. We may publish aggregate statistics that do not identify any practice, individual or patient.

9. COOKIES, ANALYTICS AND ADVERTISING

9.1 Where advertising technology is and is not used. This distinction matters, so we state it plainly:

- **Advertising and marketing cookies operate only on our public marketing pages** — the pages you can reach without logging in.
- **We do not place advertising or marketing trackers inside the logged-in Platform, in the patient portal, or on any page that displays or is tied to patient information.**

9.2 Categories we use.

Type	What it does	Can you turn it off
Strictly necessary	Authentication, session management, security, load balancing	No — the Platform will not work without these
Functional	Remembering preferences and settings	Yes

Analytics	Measuring page performance and how features are used	Yes
Advertising	Measuring marketing campaigns and showing ads on third-party sites, including social platforms	Yes

9.3 Your controls. Use the **Cookie Settings** link in our website footer to manage categories. We honour the **Global Privacy Control** signal where your browser sends it, and we treat it as a valid opt-out of advertising cookies and of sharing for cross-context behavioural advertising. Most browsers also let you block or delete cookies directly.

9.4 Do Not Track. Browsers’ “Do Not Track” signals are not standardised. We respond to the Global Privacy Control instead, as described above.

10. YOUR PRIVACY RIGHTS

10.1 Everyone. Whatever state you are in, you may ask us to access, correct or delete the personal information we hold about you as controller, and you may object to marketing at any time. Write to legal@ona.health.

10.2 If you are an Authorized User of a practice’s workspace. Your account and activity information is held within your practice’s workspace, and your practice controls it. Requests to change or remove your account should go to your practice’s administrator in the first instance. We will assist, but we will not unilaterally alter or delete records within a practice’s workspace — including audit logs, which we are required to maintain.

10.3 California residents (CCPA/CPRA). You have the right to:

- know the categories and specific pieces of personal information we have collected, the sources, our purposes, and the categories of third parties to whom we disclose it;
- delete personal information, subject to exceptions including legal retention obligations;
- correct inaccurate personal information;
- opt out of the sale or sharing of personal information — we do not sell, and the only sharing is the marketing-site advertising described in Section 9;
- limit the use and disclosure of sensitive personal information, which we use only to provide the Platform and for permitted business purposes; and
- not be discriminated against for exercising these rights.

The categories we collect, in CCPA terms, are: identifiers; commercial information; internet and network activity; approximate geolocation; professional and employment information; and inferences drawn for product and marketing analytics. We retain each category as described in Section 12. We do not knowingly collect or sell the personal information of anyone under 18.

10.4 Other state privacy laws. Residents of states with comprehensive privacy laws — including Virginia, Colorado, Connecticut, Utah, Texas, Oregon, Montana, Delaware, Iowa, Nebraska, New Hampshire, New Jersey, Minnesota and Maryland — have broadly similar rights to access, correct, delete, obtain a portable copy, and opt out of targeted advertising, sale and certain profiling. We handle all such requests through the same process.

10.5 Consumer health data (Washington and Nevada). If you are a Washington or Nevada resident, additional rights may apply to consumer health data collected through our public website. See our separate **Consumer Health Data Privacy Policy**.

10.6 Making a request. Email legal@ona.health with enough detail for us to locate your information. We will verify your identity before acting, usually by confirming control of the email address on file or by asking you to respond from your workspace account. We respond within the period the applicable law requires — generally 45 days, extendable once where permitted.

10.7 Authorised agents. You may use an authorised agent, who must provide written proof of authority. We may still contact you directly to verify the request.

10.8 Appeals. If we decline a request, you may appeal by replying to our decision with “Privacy Appeal” in the subject line. We will respond within the period the applicable law requires. If we deny your appeal, you may contact your state Attorney General.

11. SECURITY

We maintain administrative, physical and technical safeguards designed to protect personal information, including encryption in transit and at rest, role-based access control, audit logging, multi-factor authentication, least-privilege access for our personnel, vendor security review, and monitoring. Access by Ona personnel to customer environments is limited to what is necessary to provide support and is logged.

If a breach affects your information, we will notify you and, where PHI is involved, follow the process in the Business Associate Agreement and 45 CFR 164.410.

12. HOW LONG WE KEEP INFORMATION

Information	Retention
Account and practice records	For the subscription term and up to seven years afterwards, for tax, audit and legal purposes
Billing and transaction records	Seven years
Support communications	Three years from resolution
Security and audit logs	At least six years where they evidence PHI access under HIPAA
Website and analytics data	Up to 25 months

Marketing contact records

Until you opt out, then a suppression record only

Patient records are retained in accordance with the practice's instructions and our Terms of Service. On termination, a practice may export its data for **ninety (90) days**, after which we return or destroy it as the Business Associate Agreement requires.

13. NO USE BY MINORS

The Platform is business software for licensed healthcare practices. It is not offered to consumers or to anyone under 18, and no individual under 18 may hold an Authorized User credential. We do not knowingly collect personal information from anyone under 18 in our capacity as controller. Patient information about minors is PHI and is handled under the Business Associate Agreement and the practice's own policies.

14. WHERE INFORMATION IS HELD

We store and process information in the **United States**. If we change hosting region, we will give notice.

15. CHANGES TO THIS POLICY

We may update this policy. For material changes affecting practices, we will give at least **thirty (30) days'** notice by email to workspace administrators and by notice in the Platform, and we will update the version date above. Continued use after the change takes effect constitutes acceptance. We will keep prior versions available on request.

16. HOW TO CONTACT US

Ona Health Solutions Inc. 28 Geary Street, Suite 650 San Francisco, CA 94108 United States

Privacy and data protection: **legal@ona.health** Security reports: **security@ona.health**

If you are a patient, please contact the practice that treats you.