Privacy Policy
Effective Date: September 15, 2026
Last Updated: September 15, 2026

1. Who We Are

One Medical Passport Inc., doing business as One Mnet Health ("We," "Our," or "Us"), provides healthcare technology that helps patients and healthcare providers ("You") manage preoperative and medical information securely. Your privacy and the security of your information are Our highest priorities.

Because We collect and process medical information, We believe it is important for You to understand clearly how that information is used and protected. We recognize that your medical information is deeply personal, and We are committed to handling it with the highest standards of confidentiality and care.

Questions about this Policy? **Contact Our privacy team at privacy@onemnethealth.com.**

2. What This Policy Covers

This Privacy Policy ("Policy") explains what information We collect, how We use, protect, and safeguard it, and your choices as You navigate:

- The One Mnet Health Website and Web application ("Website").
- One Mnet Health mobile and desktop applications.
- Interactions with your healthcare providers.

This Privacy Policy does not apply to information collected offline or by third parties outside of Our services. We may provide additional notices for specific features or programs. By using Our services, you agree to this Policy. If You do not agree, please discontinue use. We will post updates here and change the "Last Updated" when changes are made. Your continued use of Our services after changes are posted constitutes acceptance of those changes.

3. Children's and Minors' Data

Our services are not intended for children under eighteen (18) years of age to use independently. No one under age eighteen (18) may provide any information to us without the involvement and consent of a parent, legal guardian, or authorized representative. We do not knowingly collect personal information directly from children under eighteen (18) without appropriate parental or guardian consent.

If You are under eighteen (18), do not use or provide any information on Our Website or mobile applications, including your name, address, telephone number, email address, or any username, without the involvement and consent of a parent, legal guardian, or authorized representative.

If We learn We have collected personal information directly from a child under eighteen (18) without verification of parental consent, We will delete that information promptly. If You believe We might have information from or about a child under eighteen (18) that was submitted without proper authorization, please contact Our Support team at ticket@onempcompany.com.

Note: Residents of certain states may have additional rights regarding the collection and sale of personal information of minors under thirteen (13), sixteen (16), or eighteen (18) years of age.

4. Information We Collect

We only collect what is needed to support your care and operate Our services. We collect several types of information from and about users of Our services. This section explains what We collect, how We collect it, and why.

4.1 Information You Provide to Us

When You register for an account, fill out a preoperative questionnaire, or otherwise interact with Our services, You may provide Us with the following categories of information:

Category	Examples	Shared With
Contact Information	Name, mailing address, email address, telephone number	Healthcare providers; service providers performing services on your behalf
Patient Information	Date of birth, sex, marital status, race, ethnicity, work status, occupation, primary language, religious affiliation, emergency contact, insurance information	Healthcare providers; service providers performing services on your behalf
Patient Medical Information	Medical facility name and state, surgeon name, procedure name and reason, procedure date, health history	Healthcare providers; service providers performing services on your behalf
Financial and Sensitive Personal Information	Social Security Number (collected only as required for healthcare coordination)	Healthcare providers
Online and Technical Information	IP address, browsing behavior, first-party cookies, Web server logs, activity log records	IT and security partners; fraud prevention providers; legal and compliance advisors
Compliance Data	Records of consumer preferences, including opt-ins/opt-outs, privacy rights requests, text messaging opt-in data, mobile numbers provided for messaging, and text messaging consent records	Regulators, auditors, legal counsel as required; messaging service providers, aggregators, carriers, and messaging partners as needed

		to deliver, support, and manage text messaging services

4.2 Information Collected Automatically

As You navigate through and interact with Our services, We may automatically collect certain information, including:

- Details of your visits and interactions, including traffic data, location data, logs, and other communication data.
- Information about your computer and internet connection, including your IP address, operating system, and browser type.

4.3 Cookies and Tracking Technologies

Session Cookies Only: One Mnet Health uses session-based cookies exclusively to maintain your authenticated state while You are logged in. These cookies:

- Do not store any personal information on your device.
- Are stored in temporary memory and automatically deleted when You close your browser or exit Our Website.
- Are essential for platform navigation and security.

You may refuse cookies by adjusting your browser settings. However, because Our session cookies are required for authentication, You will be unable to log in or access secure portions of Our services if cookies are disabled.

We do not collect personal information automatically through tracking technologies. We do not use persistent tracking cookies, ad networks, or retargeting tools.

5. How We Use Your Information

We use the information We collect about you, including any personal information, for the following purposes:

- Perform and provide Our services.
- To provide You with information, products, or services that You request from us.
- To fulfill any other purpose for which You provide it, such as completing preoperative questionnaires and facilitating healthcare coordination.
- To provide You with notices about your account.
- To carry out Our obligations and enforce Our rights arising from any contracts entered into between You and us, including for patient billing and collections.
- To notify You about changes to Our Website, mobile applications, or any products or services We offer.
- To allow You to participate in interactive features on Our platforms.
- To improve Our services, including analyzing usage to develop, maintain, and optimize Our platforms.
- For information security and cybersecurity purposes, including detecting threats.

- For recordkeeping, including logs and records maintained for everyday business purposes.
- In any other way We may describe when You provide the information.
- For any other purpose with your consent.

What We do NOT do: We do not collect your personal information automatically. We do not use your information for behavioral advertising unless You have provided explicit, prior consent. We do not sell, rent, share, or disclose PHI, text messaging opt-in data, mobile numbers, or text messaging consent with third parties or affiliates for their own marketing or promotional purposes. We do not share your information with third parties for their own marketing purposes. If You do not opt in (or if You later opt out), We will not use your information for behavioral advertising and will not share it with third parties for that purpose. Please visit www.mpmessages.com to Opt-out of sharing your information.

6. Who We Share Your Information With

We may disclose personal information that We collect, or that You provide, as described below:

- **Subsidiaries and Affiliates:** To Our subsidiaries and affiliates for purposes consistent with this Policy.
- **Service Providers:** To contractors, service providers, and other third parties We use to support Our business, who are bound by contractual obligations to keep personal information confidential and use it only for the purposes for which We disclose it to them.
- **Text Messaging Service Providers:** Text messaging opt-in data, mobile numbers, and text messaging consent may be shared only with service providers, aggregators, carriers, and messaging partners as needed to deliver, support, and manage Our text messaging services. We do not sell, rent, share, or disclose this information with third parties or affiliates for their own marketing or promotional purposes.
- **Healthcare Providers:** To the healthcare providers and medical facilities associated with your care, so they can access your preoperative and medical information.
- **Life Insurance and Related Coverage Requests**. At Your direction and with Your written authorization, We may disclose Your health information You authorize to a life insurance company, insurance producer, underwriting organization, medical-information service, or other recipient identified in Your authorization. These disclosures may be made to help evaluate an application for life insurance or related coverage, including eligibility, underwriting, and other purposes described in Your authorization. We disclose only the information authorized by You and only to the recipient(s) and for the purpose(s) identified in Your authorization. You may revoke an authorization in writing as permitted by law; however, revocation will not affect disclosures already made in reliance on the authorization.
- **Business Transfers:** To a buyer or other successor in the event of a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of One Mnet Health's assets, in which personal information is among the assets transferred.
- **Legal Compliance:** To comply with any court order, law, or legal process, including to respond to any government or regulatory request.

- **Rights Protection:** If We believe disclosure is necessary or appropriate to protect the rights, property, or safety of One Mnet Health, Our customers, or others.
- **With Your Consent:** For any other purpose disclosed by Us when You provide the information, or with your explicit consent.

7. HIPAA and Protected Health Information

As a healthcare technology company, certain information We process may constitute Protected Health Information ("PHI") under the Health Insurance Portability and Accountability Act ("HIPAA"). Where One Mnet Health acts as a Business Associate to a Covered Entity (such as a healthcare provider or health plan), We comply with HIPAA requirements regarding the use, disclosure, and safeguarding of PHI.

Our HIPAA compliance includes:

- Maintaining Business Associate Agreements (BAAs) with all Covered Entities We serve.
- Implementing administrative, physical, and technical safeguards as required by the HIPAA Security Rule.
- Limiting the use and disclosure of PHI to the minimum necessary for the intended purpose.
- Providing breach notification in accordance with the HIPAA Breach Notification Rule.
- Training Our workforce on HIPAA privacy and security requirements.

Your rights under HIPAA, including the right to access, amend, and receive an accounting of disclosures of your PHI, are exercised through your healthcare provider (the Covered Entity). If You have questions about how your PHI is handled, please contact both your healthcare provider and Our Privacy team at privacy@onemnethealth.com.

8. Your Privacy Rights and Choices

8.1 State Privacy Rights

State consumer privacy laws may provide residents with additional rights regarding Our use of their personal information. Residents of California, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah, and Virginia may have the following rights:

- **Right to Know/Access:** Confirm whether We process your personal data and access a copy of the personal data We maintain about you.
- **Right to Data Portability:** Receive your personal data in a portable, commonly used format.
- **Right to Delete:** Request that We delete the personal information We have collected from or about you, subject to certain legal exceptions.
- **Right to Correct:** Request correction of inaccurate personal information We maintain about you.
- **Right to Opt-Out:** Opt-out of the sale or sharing of your personal information, targeted advertising, and certain profiling.

- **Right to Limit:** Limit the use and disclosure of sensitive personal information.
- **Right to Non-Discrimination:** Not receive discriminatory treatment for exercising your privacy rights.
- **Right to Appeal:** Appeal a decision We have made in connection with your privacy rights request.

Important: The exact scope of these rights varies by state. There may also be exceptions where We are not obligated to fulfill a request.

8.2 California Residents (CCPA/CPRA)

If You are a California resident, You have additional rights under the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), including:

- The right to request categories of third parties with whom your information has been disclosed.
- The right to request removal of content (for California residents under age 18).
- **Shine the Light Requests:** The right to request information about Our disclosure of personal information to third parties for their direct marketing purposes.

For additional information, please visit Our CA Notice at Collection page at https://www.onemedicalpassport.com/app/ca-notice.

8.3 How to Exercise Your Rights

To exercise any of your privacy rights, You may:

- Email Our Privacy team at privacy@onemnethealth.com.
- Contact Our Support team at ticket@onempcompany.com.

To appeal a decision regarding a consumer rights request, You may also direct your appeal to Our Support team.

9. How We Protect Your Information

We use commercially reasonable administrative, physical, and technical measures designed to protect your personal data from accidental loss, unauthorized access, use, alteration, and disclosure. Our security program includes:

9.1 Technical Safeguards

- Industry-standard firewalls configured to allow only authorized network connections, blocking unauthorized access before it reaches sensitive systems.
- 24/7 system monitoring to ensure security protections are functioning as intended.
- All confidential information is transmitted using 256-bit SSL encryption, ensuring data is encrypted during transmission.
- Databases are not directly accessible from the internet.

- Sessions that remain inactive for 75 minutes automatically time out and require re-authentication.
- Ongoing implementation of cybersecurity best practices and risk mitigation measures.

9.2 Your Role in Security

Access to your information requires authentication using one or more secure methods supported by the platform. These methods may include password-based credentials or other authentication mechanisms that do not rely on traditional username and password. In certain cases, you may be given the option to create an account that uses a username and password. If you create login credentials, you are responsible for maintaining their confidentiality. We recommend choosing a strong, unique password. If you choose to record it, store it separately from your username and in a secure location.

While We take extensive measures to safeguard your information, no Website or electronic storage system is completely secure. We cannot guarantee the absolute security of personal information transmitted to Our services, and any such transmission is at your own risk.

10. How Long We Keep Your Information

We retain the categories of personal data described in this Policy for as long as reasonably necessary to fulfill the purposes described, or as otherwise legally permitted or required. This includes maintaining Our services, complying with legal obligations, resolving disputes, and for safety, security, and fraud prevention.

We consider Our legal and business obligations, potential risks of harm, and the nature of the information when deciding how long to retain personal data. At the end of the applicable retention period, personal data will be securely deleted, destroyed, or de-identified.

11. Correcting, Updating, or Deleting Your Information

11.1 Correcting or Updating

You may contact Our Support team at ticket@onempcompany.com to request access to, correction of, or deletion of any personal information You have provided. Please note that We may decline a request if We believe the change would violate a legal requirement or result in inaccurate information.

11.2 Removing Yourself from One Mnet Health

If You wish to have your information removed from Our systems, contact Our Support team at ticket@onempcompany.com and provide your name and username. Once your identity has been verified, We will delete your information from Our database in accordance with applicable laws and retention requirements.

12. External Links

Our services may contain links to external sites that are outside of Our control. If You follow these links, please note that those Websites may have their own privacy policies and practices, which differ from those of One Mnet Health. We are not responsible for the content, security, or privacy practices of any third-party Websites.

13. Foreign Language Support

If a language other than English is selected, the page will be translated using Google Translate. Page content is temporarily sent to Google for translation and then returned in the selected language. Google does not store or log this information. If You view the site in English, no data is transmitted to Google.

14. Changes to This Privacy Policy

We may update this Policy from time to time and will provide notice of any material changes as required by law. The date the Policy was last updated is identified at the top of this document.

We will notify You of changes by posting the updated Policy on Our Website and updating the “Last Updated” date at the top of this document. If a revised Policy becomes effective on a later date, We may also update the “Effective Date” to reflect when the revised Policy applies. We may email or otherwise communicate reminders about this Policy, but You should check Our Website periodically to see the current Policy and any changes.

15. Contact Us

To exercise your rights, ask questions, or submit comments about this Privacy Policy or Our privacy practices, contact Us at:

One Medical Passport Inc. dba One Mnet Health

Privacy Team: privacy@onemnethealth.com

Support Team: ticket@onempcompany.com

Website: https://onemnethealth.com/contact/

If You contact Us through Our online form, We will respond using the contact method You provide. We may retain your message for future reference to assist with any follow-up inquiries.