

PRIVACY POLICY

Additional Language Versions

This document is available in the following languages:

	English	https://data.my-health.today/website/en/privacy-policy.pdf
	Romanian	https://data.my-health.today/website/ro/privacy-policy.pdf
	Bulgarian	https://data.my-health.today/website/bg/privacy-policy.pdf
	Lithuanian	https://data.my-health.today/website/lt/privacy-policy.pdf
	Polish	https://data.my-health.today/website/pl/privacy-policy.pdf
	Ukrainian	https://data.my-health.today/website/ua/privacy-policy.pdf
	Hindi	https://data.my-health.today/website/hi/privacy-policy.pdf
	Russian	https://data.my-health.today/website/ru/privacy-policy.pdf
	French	https://data.my-health.today/website/fr/privacy-policy.pdf
	Arabic	https://data.my-health.today/website/ar/privacy-policy.pdf
	Brazilian / Portuguese	https://data.my-health.today/website/br/privacy-policy.pdf
	Spanish	https://data.my-health.today/website/es/privacy-policy.pdf
	Urdu	https://data.my-health.today/website/ur/privacy-policy.pdf

Important Notice: The English version of this [Privacy Policy](#) is the official and legally binding version. Translations are provided for informational purposes only. In case of any discrepancies between the translated versions and the English version, the English version shall prevail.



1. Privacy Policy & Data Protection Notice

Welcome to the H2 Platform, which includes H2 ([h2.doctor](#)) and My Health Today ([my-health.today](#)). This Privacy Policy outlines how we collect, use, and protect your personal data when you access our services.

At H2, our mission is to enhance people's well-being by delivering high-quality, accessible, and affordable healthcare through innovative and user-friendly technology.

Protecting your personal data is a key priority for us. We are committed to safeguarding your privacy and ensuring compliance with applicable data protection laws, including the UK General Data Protection Regulation (UK GDPR), the EU General Data Protection Regulation (EU GDPR), the California Consumer Privacy Act (CCPA) for US users, and, where applicable, the Health Insurance Portability and Accountability Act (HIPAA) for healthcare data in the United States. Our approach is centred on transparency, security, and putting you, our users, first.

This Privacy Policy outlines how we collect, use, and protect your personal data when you access our services, whether through H2 or one of our affiliated brands. It also applies to data collected via our website and mobile applications (the "Platform").

We encourage you to read this [Privacy Policy](#) carefully, alongside our [Terms and Conditions](#), to fully understand how your data is handled. This policy complements other notices we may provide in specific situations and does not override them.

2. Updates to This Privacy Policy & Keeping Your Information Current

We periodically review and may update this [Privacy Policy](#) to reflect changes in our practices, legal requirements, or service offerings. If significant modifications are made, we will notify you via email, platform notifications, or a public notice on our website, as required by applicable law (UK GDPR, EU GDPR, CCPA). The latest update was made on **1st April 2025**. By continuing to use our services after being notified of any updates, you acknowledge and accept the revised [Privacy Policy](#).

It is important that the information we hold about you is accurate and up to date to ensure we provide you with the best service. Please notify us promptly of any changes to your personal data during your relationship with us.

3. Third-party links

Our Platform may include links to third-party websites, plug-ins, and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their use of your personal data. When you leave our website, we encourage you to read the privacy policy of every website you visit.



4. Data Controller

In this Privacy Policy, references to 'H2-Health Help,' 'Platform,' 'H2,' 'we,' 'us,' or 'our' refer to My Health Today LTD, which operates as the data controller responsible for processing your personal data.

As part of our commitment to providing healthcare services and related products, we handle your personal data in accordance with applicable regulations. In certain cases, we may share your data with affiliated entities within the H2 Group, who act as data processors and process your information strictly under our instructions.

5. Contact Information

We have designated a Data Protection Officer (DPO) to oversee matters related to this [Privacy Policy](#). If you have any questions regarding how we handle your personal data or wish to exercise your legal rights, you can reach out to the DPO using the details below:

- Email: DPO@my-health.today
- Postal Address: **Data Protection Officer, My Health Today LTD, 7 Bell Yard, London, WC2A 2JR, United Kingdom**

If you have concerns about how your personal data is being handled, you have the right to file a complaint with the Information Commissioner's Office (ICO) in the UK (www.ico.org.uk) or the relevant data protection authority in your jurisdiction. However, we encourage you to contact us first so we can address your concerns directly.

6. Scope of Services & Regulatory Status

H2 is NOT a medical device and does not function as a regulated medical product.

H2 ([h2.doctor](#)) and My Health Today ([my-health.today](#)) provide a telehealth platform designed to facilitate virtual consultations, medical documentation, and e-prescriptions where permitted.

- H2 does not diagnose, treat, or monitor medical conditions independently.
- H2 does not provide automated or AI-generated medical decisions.
- H2 does not replace professional medical judgment or in-person healthcare.

All healthcare decisions, diagnoses, and prescriptions are made exclusively by licensed medical professionals using the platform. Any medical data processed through H2 is for facilitating patient-provider interactions only and does not constitute medical diagnosis or treatment automation.



7. How We Use Your Personal Data

We only process your personal data when permitted by law. The most common reasons for using your data include:

- Fulfilling a contract – When processing is necessary to provide the services you have requested or to take steps before entering into an agreement with you.
- Legitimate business interests – When processing supports the efficient operation of our platform, improves user experience, or ensures security, provided that your rights and freedoms do not outweigh these interests.
- Legal compliance – When processing is necessary to meet our legal and regulatory obligations.

8. Understanding Lawful Bases for Processing

Contractual necessity – We process your data when it is required to fulfil a contract you have entered into with us or when taking necessary steps before forming such a contract.

Legitimate interests – We may use your personal data to improve our services, ensure security, and manage operations. Before doing so, we carefully consider and balance your rights and interests to ensure they are not negatively impacted. Legitimate interests include, but are not limited to:

- Enhancing user experience by analyzing platform performance and engagement.
- Detecting and preventing fraudulent activities to protect users and our platform.
- Ensuring network and information security to safeguard user data from cyber threats.

Legal obligations – In certain cases, we must process your personal data to comply with applicable laws, regulations, or legal proceedings.

We adhere to the principles of data minimization and purpose limitation, meaning that we only collect and process the minimum amount of personal data required to fulfil the stated purposes. We do not retain data longer than necessary, as required by the UK GDPR, the EU GDPR, and applicable US laws (CCPA, HIPAA, where applicable).

If you have any questions regarding how we use your data, please reach out to us using the contact details provided in this policy.

9. Why We Process Your Personal Data

Below, we outline the specific purposes for which we collect and use your personal data, along with the legal grounds that justify this processing. Where applicable, we also highlight our legitimate business interests in handling your data.

Providing You with Healthcare Services

For users under the age of 16 in the EU or 13 in the US, parental or guardian consent is required before processing personal data. Where required by law, we take additional steps to ensure children’s data is handled with heightened security and privacy protection. This includes implementing age verification measures and restricting certain data-sharing activities unless explicitly authorized by a parent or guardian.

Below are the purposes for which we process your personal data and the legal bases that justify this processing.

Purpose / Activity	Legal Basis
Collecting and processing your personal data, along with that of eligible family members under 18, to manage entitlements, register accounts, and maintain medical records.	Contractual necessity
Verifying your identity and, if applicable, confirming parental responsibility for any under-18 dependents.	Legal obligation / Contractual necessity
Storing emergency contact details to ensure your safety in urgent situations.	Your consent / Vital interests
Processing financial transactions and verifying payment details for services.	Contractual necessity
Storing contact details of over 18 adults you invite to join your policy and reaching out to them for registration purposes.	Legitimate interests
Using medical information to provide effective healthcare services tailored to your needs.	Contractual necessity
Keeping a secure and detailed medical history to enable safe and efficient future healthcare services.	Legal obligation
Recording audio and video consultations with medical professionals for regulatory compliance, quality assurance, and patient safety. If recordings do not contain medical data, they may be used for training purposes with identifying details removed.	Contractual necessity
Conducting audits to ensure service quality, maintain compliance, and uphold patient safety standards.	Contractual necessity
Sharing personal data with emergency services and your designated emergency contact in urgent situations.	Your consent / Vital interests
Sending prescription details to your selected pharmacy for medication fulfilment.	Contractual necessity
With your explicit consent, share necessary medical data with your private medical insurer for claims processing and specialist referrals.	Your consent
Exchanging medical data between H2 and other healthcare professionals (e.g., GPs, hospitals, diagnostic centres, specialists) as required for your treatment.	Your consent
Providing personal data to your Healthcare Scheme to process regulatory complaints, ensuring you receive all entitled rights and protections.	Contractual necessity

Using location data during consultations to enhance safety measures, enable emergency support, and assist with selecting appropriate medical providers. Approximate location may also be derived from your IP address.	Contractual necessity
Requesting feedback on services and products to improve user experience.	Legitimate interests
Enabling our patient support team to communicate with you and provide assistance.	Contractual necessity
Sharing relevant personal data (excluding medical data unless consented) with your healthcare scheme to verify eligibility, registration status, and billing details, as well as processing service terminations.	Contractual necessity

Keeping You Informed

We process your personal data to provide you with important updates and communications. Below are the purposes and legal bases for these activities.

Purpose / Activity	Legal Basis
Sending activation instructions via email to help you access and use the platform benefits.	Contractual necessity
Delivering essential service notifications via email, SMS, WhatsApp, or push notifications, such as confirmation of account activation, appointment reminders, triage updates, and availability of medical documents (e.g., prescriptions, referrals, test results).	Contractual necessity
Occasionally send promotional emails about our services, provided you have not opted out. You can adjust your preferences anytime in your account settings.	Legitimate interests
Contacting you via email, phone, mail, or push notifications with special offers or service updates, but only if you have explicitly opted in. You may change your communication preferences at any time.	Consent

Research and Analytics

We process certain data to enhance our platform, improve healthcare services, and support business operations. Below are the purposes and legal justifications for these activities:

Purpose / Activity	Legal Basis
Analyzing anonymized medical data to enhance healthcare delivery, refine our products, and improve overall patient care. All personal identifiers (e.g., name, email, address, phone number) are removed to protect privacy.	Legitimate interests
Assessing how users interact with the platform to identify areas for improvement, address technical issues, and optimize functionality.	Legitimate interests

Evaluating user engagement and behaviour to enhance platform design, accessibility, and service offerings.	Legitimate interests
Tracking demand trends for services and features to plan resources efficiently and meet user needs.	Legitimate interests
Conducting demographic research to better understand user needs and tailor our services accordingly.	Legitimate interests
Sharing aggregated and anonymized insights with healthcare schemes to support service improvements, ensuring no personally identifiable information is disclosed.	Legitimate interests

When We Are Required to Use Your Personal Data

In certain situations, we may need to process your personal data to meet legal, regulatory, or public interest requirements. Below are the purposes and legal justifications for these activities:

Purpose / Activity	Legal Basis
Collaborating with regulatory bodies, including the Care Quality Commission (CQC), General Medical Council (GMC), Information Commissioner's Office (ICO), or other relevant authorities as required by law.	Legal obligation
Complying with legal requirements such as court orders, law enforcement requests, or statutory obligations.	Legal obligation
Managing and responding to legal claims, regulatory investigations, or dispute resolution processes.	Legal obligation
Taking necessary actions to address public health risks and ensure compliance with government-mandated health and safety measures.	Public task
Sharing your personal and medical data with your insurance provider, but only when explicitly instructed by you or your insurer.	Your consent

Providing Accurate and Up-to-Date Information

We require accurate and up-to-date personal data to ensure we can effectively deliver our services and comply with legal and contractual obligations. If you fail to provide the necessary information when requested, we may be unable to offer certain services. In such cases, we will notify you if any restrictions or cancellations apply.

We take reasonable steps to keep your personal data accurate, but it is ultimately your responsibility to ensure that the information stored on the H2 Platform is correct and up to date. We are not liable for any issues resulting from inaccurate data that you have provided, including errors affecting service delivery or communications.

10. Categories of Personal Data We Collect

We collect and process different types of personal data as part of your patient record on the H2 Platform. We adhere to the principles of data minimization and purpose limitation, meaning that we only collect and retain the data strictly necessary for the purposes stated in this Privacy Policy. Personal data is not used for secondary purposes unless explicitly consented to by the user.

1. Identity Data

When registering, you will be asked to provide personal details, which may include:

- Full name, date of birth, email address, phone number, and postal address.
- Profile photo and healthcare identification number (if applicable).

To enhance security, we may verify your identity through documents such as passports or driving licenses. This verification is conducted either by our in-house team or trusted third-party providers, all of whom are bound by confidentiality obligations. A live photo may be used as your profile image to ensure account security.

For identity verification, we may process biometric data, such as facial recognition images, through trusted third-party providers. This data is processed strictly for verification purposes and is not stored by H2 beyond the verification process. Our verification partners are contractually required to comply with UK GDPR, EU GDPR, and applicable US laws (CCPA, HIPAA where relevant).

Additional information, including proof of parental responsibility, is required for users adding dependents under 18. If you invite an adult (over 18) to join your policy, their name, email, and date of birth will be collected.

Additionally, any correspondence you have with our patient support team (via email, phone, or chat) may be recorded and securely stored for service quality, training, and regulatory compliance.

Lawful basis for processing identity data:

- Contractual necessity (when verifying identity and maintaining account security).
- Legitimate interest (when using identity data for fraud prevention).

2. Medical Data

Providing medical data is voluntary; however, choosing not to share relevant details may limit our healthcare partners' ability to offer certain healthcare services.

- You may update your medical record via the H2 Platform, and once verified during a consultation, this data will become part of your permanent record.
- When booking an appointment, you may be required to provide details about your health concerns, symptoms, and relevant medical history.

- During consultations, our medical professionals will document your symptoms, health conditions, family history, allergies, prescribed treatments, and referrals as part of your patient record.
- Uploaded documents, photos, and test results may also be included in your record, as determined by our medical professionals. If an uploaded file is deemed unnecessary for long-term medical documentation, it will be removed.
- Laboratory and diagnostic test results (e.g., blood tests, imaging scans) will be securely stored, and a specialist report will be prepared as part of your care.

To maintain regulatory and safety standards, we may record video and audio consultations with healthcare professionals. These recordings are securely stored for monitoring service quality, patient safety, and compliance with healthcare regulations.

All medical data is stored in secure, encrypted databases.

Lawful basis for processing medical data:

- Contractual necessity (when providing healthcare services).
- Legal obligation (for regulatory compliance).
- Explicit consent (when sharing data with external providers or insurers).

Translation Disclaimer & Limitations

AI-powered translations of medical documents (including prescriptions, medical consultation summaries, diagnoses, and referrals) are provided for informational purposes only. While we strive for accuracy, H2 cannot guarantee 100% precision in automated or human-reviewed translations.

These translated versions do not replace the original medical documentation issued during your consultation and should not be solely relied upon for medical, legal, or regulatory purposes.

It is your responsibility to verify the accuracy and appropriateness of any translated document before presenting it to local authorities, healthcare providers, or third parties.

H2 is not liable for any misunderstandings, misinterpretations, or outcomes resulting from translated documents.

3. Health Monitoring and Connected Devices

If you use health-tracking features within the H2 Platform, any medical or wellness data you provide will be processed as part of your patient profile.

Additionally, if you choose to integrate third-party apps or smart devices (e.g., fitness trackers, smartwatches, or connected health applications), we may collect health-related data from these sources only with your explicit consent.

Data collected from health-tracking apps or connected devices is processed only with your explicit consent, as required under GDPR Article 9 for special categories of data and HIPAA for US users.

We ensure that all data processing adheres to GDPR requirements and follows strict security protocols to protect your privacy.

11. Financial Data

If you choose to use pay-as-you-go or subscription-based services, your payment details (such as debit/credit card information) will be processed by a secure third-party payment provider. All transactions are handled on their servers, ensuring compliance with industry security standards (PCI DSS).

H2 does not store your card details on the platform. Lawful basis for processing financial data: Contractual necessity (to process payments securely).

12. Technical Data and Analytics

To enhance security and improve user experience, we collect certain technical data, which may include:

- Login credentials are stored securely, with users responsible for maintaining password security.
- Device and connection details, including IP address, operating system, browser type, time zone, and mobile carrier (where applicable).
- Usage patterns, such as interactions with features, page visits, and engagement with platform services.

This data is only collected with your consent and is used to improve the platform, troubleshoot technical issues, and optimize functionality.

13. Cookies and Tracking Technologies

We use cookies to enhance your browsing experience by storing preferences and tracking interactions on our platform. These small data files allow us to:

- Analyze website traffic and improve navigation.
- Remember user settings and preferences for future visits.
- Provide secure login sessions.

We do not use cookies to process sensitive medical or health-related data. For more details on how we use cookies and how you can manage your preferences, refer to our [Cookie Policy](#).

14. Data from Third Parties

If you receive services through a healthcare scheme, we may collect and store certain personal details provided by your scheme to facilitate account activation and benefit eligibility verification. This may include:



- Membership ID, name, date of birth, email, and postal address.
- Healthcare identification number and registered GP details, retrieved from national databases such as the NHS Personal Demographic Service (where applicable).
- Medical referral or claim status updates from private insurers when you request a referral or submit a claim.

Additionally, we may receive diagnostic results or specialist reports from healthcare providers involved in your treatment.

15. Data Sharing and Third-Party Access

We prioritize your privacy and security and only share your data when necessary, legally justified, and in compliance with applicable regulations. All external partners must adhere to strict confidentiality agreements, process data solely for specified purposes, and comply with GDPR, CCPA, and HIPAA (where applicable).

If you are a California resident or reside in another jurisdiction with data opt-out rights, you may request that we restrict certain types of data sharing with third-party providers. To exercise this right, contact our Data Protection Officer (DPO) at DPO@my-health.today.

Who We Share Data With:

- Contracted Service Providers – We work with trusted third-party vendors for essential services such as identity verification, payment processing, and communications. These providers process data only under our strict instructions and are bound by GDPR's Article 28 contracts.
- Regulatory Bodies & Authorities – We may share personal data with entities such as the Care Quality Commission (CQC), General Medical Council (GMC), Information Commissioner's Office (ICO), NHS Digital, and US regulatory bodies under HIPAA and CCPA as required for regulatory compliance and patient safety.
- Identity Verification Providers
- Communication & Storage Partners – Some video, phone, text, and email interactions may be temporarily stored on secure servers outside the UK and EEA while being processed. These transfers comply with GDPR Standard Contractual Clauses (SCCs), CCPA, and HIPAA requirements where applicable.
- Payment Provider (Stripe) – To process payments, financial details are encrypted and processed directly through Stripe (based in the USA). We do not store credit or debit card details on our servers.
- Healthcare Professionals – Your medical data is securely shared with licensed doctors, specialists, and pharmacists registered with the UK General Medical Council (GMC), or other recognized local medical boards.

16. Research and Medical Insights

We may use anonymized and aggregated medical data for research and service improvements. This data is fully de-identified to ensure it cannot be traced back to individual users in compliance with GDPR, CCPA, and HIPAA requirements.

If H2 undergoes restructuring, acquisition, or merger, your personal data may be transferred to the new entity, subject to continued compliance with this Privacy Policy.

We may also be legally required to disclose personal data to prevent fraud, and cybercrime, or to comply with court orders.

17. Sharing Data with Healthcare Providers

For the provision of medical care, we may securely share relevant personal and medical data with:

- Your GP and other healthcare professionals are involved in your treatment.
- Pharmacies to facilitate prescription fulfilment.
- Hospitals, diagnostic centres, and emergency services to support continuity of care and urgent medical needs.

These providers may contact you directly regarding appointments, medications, or follow-up care.

18. Your Data Security and Rights

We implement industry-standard encryption and strict access controls to safeguard your personal data.

You have the right to:

- Access Your Data – Request a copy of your personal data.
- Request Corrections – Rectify inaccurate or outdated data.
- Withdraw Consent – Revoke previously granted consent where applicable.
- Object to Processing – Restrict certain types of processing based on legitimate interests.
- Request Data Deletion – Request removal of your personal data (subject to legal limitations).

For inquiries about your privacy rights, contact our Data Protection Officer (DPO) at DPO@my-health.today.

19. Protecting Your Privacy

Your privacy is our priority, and we only share personal data when necessary and in compliance with applicable laws. We require all third-party providers to adhere to strict security and confidentiality agreements, ensuring that your data is only processed for specified purposes.

20. How We Share Your Data

- H2 Group Partners – Data may be shared within H2 Group to provide services efficiently.

- Service Providers—We collaborate with carefully selected identity verification, payment processing, and communication service providers, which are contractually bound by GDPR Article 28 agreements.
- Regulatory Authorities – Data may be shared with CQC, GMC, ICO, NHS Digital, and HIPAA-regulated US entities for compliance and patient safety.
- Identity Verification Services
- Communication & Hosting Services – Some video, phone, and text interactions may be processed on secure servers outside the UK and EEA. All transfers comply with GDPR Standard Contractual Clauses (SCCs).
- Payment Processing – All transactions are encrypted and processed securely through Stripe. We do not store credit or debit card details.
- Healthcare Professionals – Your medical data is securely shared with licensed professionals only when necessary for treatment.

21. Healthcare Providers and Insurance Schemes

If required for treatment, we securely share relevant medical data with:

- GPs, hospitals, pharmacies, and emergency services.
- Healthcare schemes, where non-medical data (e.g., name, date of birth, and eligibility details) may be shared for registration and billing purposes.
- Private insurers to process medical referrals and claims, but only with your explicit consent.

22. Data Anonymization for Research & Analytics

- We may use anonymized and aggregated data for research, business insights, and healthcare improvements.
- Identifiable information (e.g., name, email, phone number) is always removed before analysis.

23. International Data Transfers

Whenever personal data is transferred outside the UK and EEA, we ensure compliance with GDPR, CCPA, and HIPAA through legally recognized safeguards, such as:

- Standard Contractual Clauses (SCCs) approved by regulatory authorities.
- Data Processing Agreements (DPAs) with international partners.
- Alternative mechanisms such as Privacy Shield frameworks (where applicable).

Your data is stored within UK and EEA-based secure data centres unless a legally justified transfer is necessary.

24. Data Retention Periods

We retain personal data only as long as necessary to fulfil the purposes outlined in this policy:

- Medical Records – Up to 10 years after the patient’s passing, in line with healthcare regulations.
- Call Recordings – Stored for 12 months for quality monitoring and compliance.
- Identity Verification Documents – Retained for 60 days post-verification.
- Inactive Accounts – If you register but never activate, your data is retained for up to 2 years (or 7 years if you were once eligible for a benefit but never used the service).

25. Data Security Measures

To prevent unauthorized access, misuse, or loss, we have implemented:

- End-to-End Encryption for data storage and transmission.
- Regular Security Audits & Penetration Testing to identify vulnerabilities.
- Strict Access Controls limiting data access to authorized personnel.
- Multi-Factor Authentication (MFA) and strong password enforcement to secure accounts.
- Real-time Monitoring for cybersecurity threats.

26. Your GDPR Rights

Your Data Protection Rights

Under UK GDPR, EU GDPR, and US laws (CCPA, HIPAA where applicable), you have the following rights:

- Right to Access – Request a copy of the personal data we hold about you.
- Right to Rectification – Correct inaccurate, outdated, or incomplete data.
- Right to Erasure ("Right to Be Forgotten") – Request deletion of your personal data, subject to legal obligations (e.g., medical records may need to be retained for compliance with healthcare regulations).
- Right to Restrict Processing – Request that we temporarily stop processing your data under specific circumstances, such as when disputing data accuracy or objecting to processing.
- Right to Data Portability – Request to receive your data in a structured, commonly used, and machine-readable format or transfer it directly to another service provider.
- Right to Object – Object to processing based on legitimate interests, direct marketing, or automated decision-making.
- Right to Withdraw Consent – If processing is based on consent, you have the right to withdraw it at any time without affecting prior lawful processing.
- Right to Challenge Automated Decision-Making and Profiling – Request human intervention if a decision significantly affects you based on automated processing.

For California residents under CCPA, additional rights include:

- Right to Opt-Out of Sale or Sharing of Personal Data – You may request that we do not sell or share your personal data with third parties.
- Right to Limit Use of Sensitive Personal Information – You may request that we restrict how sensitive personal information (e.g., medical data) is used beyond providing the requested services.
- Non-Discrimination – We will not deny services, charge different prices, or offer a different level of service due to the exercise of your rights.

For US users covered by HIPAA, medical data is handled in accordance with HIPAA Privacy and Security Rules, which govern access, disclosure, and security of Protected Health Information (PHI).

Exercising Your Rights

To exercise your rights, you may contact our Data Protection Officer (DPO):

- Email: DPO@my-health.today
- Postal Address: Data Protection Officer, My Health Today LTD, 7 Bell Yard, London, WC2A 2JR, United Kingdom

We may ask for identity verification before fulfilling your request to ensure the security of your personal data. If you are making a request on behalf of another individual, we may require proof of authorization.

For California residents, you may submit a CCPA-related request by contacting us at DPO@my-health.today or through any methods required by applicable laws.

27. Data Breach Notification Compliance

*In the event of a data breach that poses a risk to your rights and freedoms, we will notify you and the appropriate regulatory authority within the legally required timeframe. This includes:**

- UK GDPR & EU GDPR – Notification within 72 hours to the ICO (UK) or relevant Data Protection Authority (EU).
- CCPA (California Residents) – Notify affected users within a reasonable timeframe.
- HIPAA (US Healthcare Data Breach Notification Rule) – Notification within 60 days to affected individuals, the US Department of Health & Human Services (HHS), and, if applicable, media outlets (for breaches affecting over 500 individuals)

28. Response Time

We aim to process all requests within one month as required by UK GDPR, EU GDPR, and CCPA. However, if the request is complex or requires additional verification, we may extend this period by an additional two months. If an extension is required, we will notify you of the reason and expected timeframe.

Responses to HIPAA-related data requests will be provided within 30 days unless an extension is necessary under HIPAA Privacy Rule standards.



If you have concerns about how your data is handled, you may also file a complaint with:

- UK Information Commissioner's Office (ICO): www.ico.org.uk
- EU Data Protection Authorities (DPA): www.edpb.europa.eu
- California Attorney General (for CCPA complaints): www.oag.ca.gov/privacy/ccpa
- US Department of Health & Human Services (for HIPAA complaints): www.hhs.gov/hipaa

However, we encourage you to contact us first so we can address your concerns directly.