# Merlin Health Privacy Policy

*This Notice is effective December 15, 2017.*

By reviewing and accepting the practices outlined in this notice, and any subsequent changes, you agree that you have been notified of the ways we collect, use and disclose your personal medical records, protected health information ("PHI"), and other personal information, and how you can request access to our records containing your PHI. This is an important agreement between you, your healthcare providers, us, and our partners ("Business Associates"), and we take it very seriously. We are committed to maintaining your privacy and we have implemented policies and technology to ensure your PHI is secure.

Your rights and our obligations are governed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and associated Privacy and Security rules established by the United States Department of Health and Human Services ("HHS"). More information can be found at the HHS HIPAA website at https://www.hhs.gov/hipaa/for-individuals/index.html

## PHI Defined

HHS defines PHI as information that identifies you, such as name, address, birth date, or Social Security Number, and relates to your past, present or future physical or mental health or condition; the provision of health care to you; or the past, present, or future payment for the provision of health care to you.

## How we collect your PHI and other personal information

Our record of your PHI is generated from a combination of information entered by you upon registering an account, creating a health profile or timeline, or otherwise interacting with the Merlin™ application and services, as well as any health information entered by your healthcare provider(s), and any other documents uploaded by you.

We also may collect information automatically about you, including, but not limited to: log information collected by our servers that may contain your IP address, geo-location, operating system, and device keys or other details. We utilize information collected from tracking technologies to understand your use of our services, with the intention of improving and maintaining our service and interacting with you in more meaningful ways.
We may also obtain other personal information about you from public databases, use of our social media sites, and our Business Associates, and other third-party sources.

## How we use and disclose your protected health information

HIPAA rules permit Merlin Health and our Business Associates to use and disclose your protected health information for purposes of treatment, payment, and healthcare operations, defined as follows.

**Treatment**
Treatment is the provision, coordination, or management of health care and related services for you by one or more health care providers, including consultation between providers about you and referral by one provider to another for your care.

**Payment**
Payment encompasses activities of obtaining premiums, determining or fulfilling responsibilities for coverage and provision of benefits, and furnishing or obtaining payment or reimbursement for health care delivered to you, and related activities, when applicable.

**Health care operations**
Health care operations are any of the following activities: (a) quality assessment and improvement activities; (b) competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation; (c) conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; (d) specified insurance functions, such as underwriting, risk rating, and reinsuring risk; (e) business planning, development, management, and administration; and (f) business management and general administrative activities, including but not limited to: de-identifying protected health information, creating a limited data set, and certain fundraising.

Any third party required in the delivery of services will be required to comply with this Privacy Policy and associated HIPAA rules, and will be required to sign a Business Associate Agreement documenting their obligations to protect your PHI.

**Legal Compliance**
We may use and disclose your PHI to comply with federal and state laws, including, but not limited to:

- Court or Administrative Agency orders, or in response to a subpoena
- Law enforcement requests, such as information about a victim or suspected victim of a crime; suspicion of domestic violence, child abuse or neglect; or identifying or locating a suspect, fugitive, material witness, or missing person.
- Federal official requests for intelligence and national security purposes
- FDA reporting on public safety issues
- Complying with workers' compensation issues, as required under OHSA or other state laws
- Health oversight agencies for authorized audits and investigations

**Public & Community Health**
For national priority purposes related to protecting the public, we may under special circumstances disclose your PHI to public health authorities authorized by law to collect or receive such information for preventing or controlling disease, injury, or disability. When notification is authorized by law, we may disclose your PHI to anyone who may have been exposed or be at risk of contracting or spreading a communicable disease.

**Marketing**
We may collect, use, and disclose your PHI for the purposes of permitted marketing activities, as follows:

- Communications for your treatment
- Communications to describe health-related products or services, or payment for them, provided by us or our Business Associates
- Communications for case management or care coordination for you, or to recommend alternative treatments, therapies, health care providers, or care settings to you.

**With Your Authorization**
Any other use or disclosure of your PHI will only occur with your written (electronic) authorization, for specific conditions as authorized by you. You may revoke your authorization at any time by emailing us at help@hellomerlin.io.

**De-identified Information**
We may use De-Identified Information created by us without restriction.

## Your Rights Under HIPAA

**Access to your PHI**
You have the right to review and obtain a copy of our records containing your protected health information, that are used to make decisions about you. We may under law deny access in certain specified situations, such as when a health care professional believes access could cause harm to you or another individual. You will be given the right to have such denials reviewed by a licensed health care professional for a second opinion. You also have the right to request a paper copy, for which we may impose reasonable fees for the cost of copying and postage if applicable.

**Amendment to your PHI**
You have the right to request that we amend your protected health information in our records when that information is inaccurate or incomplete, and we will make reasonable efforts to provide the amendment to persons that you have identified as needing it, and to persons that we know might rely on the information. If the request is denied, we will provide you with a written denial, in which case you may submit a statement of disagreement for inclusion in the record.

**Disclosure Accounting**
You have a right to an accounting of certain disclosures of your protected health information by us or our business associates. The maximum disclosure accounting period is the six years

immediately preceding your request. However, in alignment with HHS HIPAA rules, we may not provide accounting for the following permitted disclosures:

(a) for treatment, payment, or health care operations;
(b) to you or your personal representative;
(c) for notification of or to persons involved in your health care or payment for health care, for disaster relief, or for facility directories;
(d) pursuant to an authorization;
(e) of a limited data set;
(f) for national security or intelligence purposes;
(g) to correctional institutions or law enforcement officials for certain purposes regarding inmates or individuals in lawful custody; or
(h) incident to otherwise permitted or required uses or disclosures.

**Restriction Request**

You have the right to request that we restrict use or disclosure of protected health information for treatment, payment or health care operations, disclosure to persons involved in your health care or payment for health care, or disclosure to notify family members or others about your general condition, location, or death. We are under no obligation to agree to requests for restrictions, and will consider each case individually, and we will continue to be obligated to comply with laws and regulations.

**Confidential Communications**

You may request an alternative means or location for receiving communications of protected health information, such as through a designated email address or phone number. It is however your responsibility to maintain the privacy of and access to your mobile device, and our mobile application allows you to turn off notifications at any time. Device notifications or text ("SMS") messages from us will never contain any protected health information, and you will be required to authenticate through the mobile application before accessing your PHI. We will accommodate reasonable requests if you indicate that the disclosure of all or part of the protected health information could endanger you, and if requested in writing. If accepted, we will notify you of any impact to the Services we provide based on your request (for example, if a phone number you have requested us to contact you does not match the number registered to the device associated with the download of our mobile application). More information on our use of Electronic Communications can be found in our Terms of Service.

**Breach Notification**

You have the right to be notified of a breach resulting in unsecure access to your PHI without unreasonable delay and in no case later than 60 days following the discovery of a breach. We will send notifications to your email address in your account profile. If we cannot reach you by email we will make a reasonable effort to notify you of the breach via other means.

## Further Information and Complaints

If you would like more information about your privacy rights, you may email us at help@hellomerlin.io. If you believe that your privacy rights as defined in HIPAA have been violated, you must write us at Merlin Health LLC, Attention: Privacy Officer, 5601 Democracy Dr, Suite 250, Plano TX 75024. You may also learn more and file a complaint with HHS at https://www.hhs.gov/hipaa/filing-a-complaint/index.html

## Changes to this Privacy Policy

Any changes to this policy will apply retroactively to all protected health information we have collected and maintain, and will be posted to our website at www.merlin.health, and updated in the Merlin™ mobile application, requiring your acceptance for continued use of our Services as defined in our Terms of Service.