FLATIRON HEALTH PHI PRIVACY NOTICE

Effective Date: May 5, 2026

TABLE OF CONTENTS

---

1. OVERVIEW

The privacy policy below (the "**Notice**") applies to patient users of Flatiron Health products such as the patient portal CareSpace and services that Flatiron Health provides on behalf of its HIPAA-regulated customers (your healthcare provider). For our privacy policy related to our website and other Flatiron products and services, please review our **General Privacy Notice and Cookie Policy**.

2. PROVIDER AGREEMENTS AND YOUR HEALTH-RELATED INFORMATION

Flatiron Health, Inc. (**"Flatiron," "we," or "us"**) provides electronic health record (**"EHR"**) services, patient portals, and other services (collectively **"Services"**) to health care provider customers (**"Provider Customers"**) under agreements with the Provider Customers that govern our use and disclosure of their patients' (as defined below) and other Personal Information through the Services (**"Provider Agreements"**). This Notice supplements those Provider Agreements. To the extent that a term of this Notice conflicts with any applicable Provider Agreement, the Provider Agreement will control.

In the performance of the Services, Flatiron may collect electronic health record information, including Protected Health Information or "**PHI**", which is defined as personally identifiable health information protected by the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (**"HIPAA"**). Included in your PHI may be other sensitive categories of information such as your race, gender, sexual orientation or preferences, and biometrics. We collect this information for the

purposes of providing the Services to our Provider Customers and may also create de-identified or aggregated datasets derived from PHI for research purposes as described below and as permitted under the applicable Provider Agreement and HIPAA. We only use the PHI as permitted under the applicable Provider Agreement and applicable law.

As between Flatiron and our Provider Customers, our Provider Customers are responsible for determining how we use and disclose the PHI we collect through the Services. Your healthcare provider's collection, use, and disclosure of information about you is governed, in turn, by your provider's own notice of privacy practices, privacy policies and terms and conditions.

If you are a patient of one of our Provider Customers using a patient portal or other Service provided under a Provider Agreement and have questions about your treatment or handling of your health-related information, you should check with your healthcare provider. If you would like to request changes to your PHI that your healthcare provider stores in our EHR systems or uses in connection with the Services, please contact your healthcare provider directly.

3. WHAT PERSONAL INFORMATION WE COLLECT AND ITS SOURCE

When you interact with us, we may collect the following Personal Information:

- Direct identifiers, such as your name, address, email address, telephone number, or an IP address or other online identifier. We typically collect this information directly from you in order to communicate with you and provide you with access to certain information on our Sites or about our services.

- Internet activity information, such as your browsing history, search history, and browser information as it relates to the use of our Sites or other services. We typically collect this information from our use of cookies and other data collection technologies to help us design our website, to identify popular features, and for other managerial purposes. You can review our Cookie Notice here.

- Location information, which is used to locate the device you use to access our Sites. Location information may include: (i) the location of the device derived from GPS or WiFi use; (ii) the location derived from the IP address of the device or internet service used to access the Sites; and (iii) other information made available by a user or others that indicates the current or prior location of the user.

- Profile information, such as information about your preferences and characteristics. We typically collect this information directly from you and through our use of cookies and other data collection technologies in order to tailor our services and communications to you. Usage information, such as information about how you use our Services and how you navigate our site. This information

is collected automatically as you interact with our Services through your device or through third-party cookies. The information we automatically collect includes data about your device (for example, device ID, browser type), IP address, information about when you accessed or registered, modified, logged in/out of the Services information related to actions taken on the site and information related to your operating system.

- **The Personal Information collected for our patient-facing products are solely for the purpose of providing our services to you (e.g. the provision of cancer care) and for our business operations (e.g. for the identification of bugs or unsafe internet traffic).**

We may also collect non-identifiable information, such as the type of browser or operating system you are using. We may also de-identify or anonymize your Personal Information in accordance with applicable law or create aggregate, anonymized information that relates to a group of individuals, which we may use for any lawful purpose in accordance with applicable law.

Note that we do not use non-health related Personal Information, such as IP addresses or search history, to infer specific health conditions or medical statuses of our users unless such processing is strictly necessary to provide the requested Service.

4. PURPOSE FOR COLLECTION

In addition to the purposes for collection listed above, we may also collect each of the above categories of Personal Information in order to provide you services and for our own internal business purposes, which include:

- Fulfilling your requests, including to register and administer your account and provide you the information, products and services that you request (including, where applicable, user activities associated with the licensing and use of Flatiron tools and services such as user authentication and credentialing).

- Improving our Site and services, such as by improving the content, features and functionality of our Site and services, identifying popular features, and enabling more accurate reporting.

- As otherwise may be disclosed to you at the time of collection.

5. HOW WE SHARE YOUR PHI

We may share your Personal Information for the reason(s) disclosed to you at the time we collect it, with your consent, at your direction, or in the following ways:

- **Within Flatiron:** We may share your Personal Information internally among the Flatiron subsidiaries (e.g. Flatiron US, Flatiron UK, Flatiron Germany, and Flatiron Japan) in order to provide you our services and generally improve our product and service offerings.

- **With vendors and other service providers**: We may share your Personal Information with service providers who perform services for us and act on our direction. These services may include activities such as IT services. Flatiron enters into appropriate contractual arrangements, called Business Associate Agreements, with any service providers who will access your PHI to obtain the requisite assurances that your health information will be accessed securely and only for the purposes of providing services to you or as otherwise permitted or required by law.

- **To comply with our legal obligations and to protect our rights**: We will disclose your Personal Information when we think it is necessary to investigate or prevent actual or expected fraud, criminal activity, injury or damage to us or others or when otherwise required by statute, regulation, subpoena, court order, or other law, or if necessary to protect the rights, property, or safety of us, our employees, or others.

6. HOW LONG WE RETENTAIN YOUR INFORMATION

We will only retain your Personal Information for as long as necessary to fulfill the purposes for which it was collected and processed, including for the purposes of satisfying any legal, regulatory, accounting or reporting requirements. We will also retain and use your Personal Information to the extent necessary to resolve disputes and enforce our terms and conditions, other applicable terms of service, and our policies.

To determine the appropriate retention period for your Personal Information, we will consider the amount, nature, and sensitivity of the data, the potential risk of harm for unauthorized use or disclosure, the purposes for which we process it and whether we can achieve those purposes through other means, and the applicable legal requirements.

Upon expiration of the applicable retention period, we will securely destroy your personal data in accordance with applicable laws and regulations.

7. YOUR PRIVACY CHOICES REGARDING YOUR PHI

As described in greater detail in Section 1 (“Provider Agreements and Your Health-Related Information”), requests regarding your PHI must be directed to your healthcare provider. As described in greater detail in Section 10 (“Our Clinical Research Offerings) requests regarding your PHI or other Personal Information collected in the context of a clinical study in which Flatiron’s Clinical Research Offerings are utilized must be

directed to the study sponsor or the clinical research organization that is responsible for the study or your study healthcare provider. Although Flatiron is not required to provide you with a HIPAA Notice of Privacy Practices (as we are a Business Associate and not a Covered Entity), you have important rights under HIPAA regarding your PHI:

- Right to Access: Inspect and obtain copies of your PHI.
- Right to Amend: Request corrections to your PHI.
- Right to an Accounting: Receive an accounting of certain disclosures.
- Right to Request Restrictions: Request restrictions on certain uses and disclosures.
- Right to Confidential Communications: Request communications by alternative means or at alternative locations.
- Right to a Copy of Notice: Obtain a paper copy of your healthcare provider's Notice of Privacy Practices.
- Right to Breach Notification: Be notified of breaches of your unsecured PHI.
- Right to File a Complaint: File a complaint with your healthcare provider, the HHS Office for Civil Rights, or Flatiron if you believe your privacy rights have been violated.

How to exercise your HIPAA rights: Because Flatiron processes your PHI on behalf of your healthcare provider, requests to exercise HIPAA rights must be directed to your healthcare provider. Your healthcare provider's Notice of Privacy Practices will explain how to exercise these rights.

You have the right to opt-out of Flatiron's use of your information for research purposes. See Section 11("How Patients Contribute to Research") below for details.

8. CALIFORNIA RESIDENTS' PRIVACY RIGHTS

Applicability: This sub-section (f) applies to California residents and supplements the information in this Notice.

Categories of Personal Information Collected: In the preceding 12 months, we have collected the following categories of Personal Information: identifiers (name, address,

email, IP address), internet activity information (browsing history, browser information), geolocation data, and profile/preference information.

We do not "sell" or "share" Personal Information as those terms are defined by the California Consumer Privacy Act (CCPA).

We collect PHI, which the CCPA categorizes as "sensitive personal information." We use and disclose this sensitive personal information only:

- To provide healthcare services through our Provider Customers;
- For healthcare operations as permitted under our Provider Agreements;
- To create de-identified research datasets as described in this Notice; and
- As otherwise permitted by HIPAA and our Provider Agreements

California residents have the right to:

- Know what Personal Information we collect, use, disclose, and sell;
- Access your Personal Information (up to twice per 12-month period);
- Delete your Personal Information, subject to certain exceptions;
- Correct inaccurate Personal Information;
- Limit the use and disclosure of sensitive personal information;
- Opt-out of the sale or sharing of your Personal Information (though we do not sell or share); and
- Non-discrimination for exercising your privacy rights.

How to Exercise Your Privacy Rights:

- For PHI collected through our Services on behalf of your healthcare provider, please contact your healthcare provider directly. For any other Personal Information or privacy-related inquiries, or to exercise any of your privacy rights listed above: Email privacy@flatiron.com or call 888-662-6367.

- We will verify your identity before responding to any of your inquiries. We may request information such as your name, email, and information about your

interaction with us. We may decline a request if we cannot verify your identity or if an exception applies.

- We will respond to verifiable requests within 45 days. If we need more time (up to 90 days total), we will inform you of the reason and how much additional time we need.

- You may designate an authorized agent to make requests on your behalf. We will require written proof that the agent is authorized to act on your behalf or a valid power of attorney.

- We will never discriminate against you for exercising your CCPA rights.

9. OTHER US STATES' PRIVACY RIGHTS

Residents of other US states, such as Virginia, Colorado, Connecticut, Utah, Montana, Oregon, Texas, and Delaware, also have privacy rights under their respective state privacy laws. These rights generally include rights to:

- Access, delete and obtain a copy of your Personal Information.
- Correct inaccurate Personal Information.
- Opt-out of the sale of Personal Information or targeted advertising (note that we do not sell Personal Information or engage in targeted advertising as defined by these laws).

To exercise any of your privacy rights under your state's privacy law, please contact us at privacy@flatiron.com or call us at 888-662-6367.

10. OUR CLINICAL RESEARCH OFFERINGS

Flatiron provides clinical research support offerings (**"Clinical Research Offerings"**) to clinical trial sponsors, contract research organizations, functional service providers, and health systems (collectively **"Clinical Research Customers"**). Our agreements with the Clinical Research Customers govern our collection and use of Personal Information that we collect in connection with our Clinical Research Offerings (**"Clinical Research Offerings Agreements"**).

Our Clinical Research Customers are responsible for determining how we can use the Personal Information we collect through the Clinical Research Offerings.

If you are a participant in a clinical study in which Flatiron's Clinical Research Offerings are utilized and you have questions about the study or how Personal Information is

handled, you should consult with the study sponsor or the clinical research organization that is responsible for the study or your study healthcare provider.

11. HOW PATIENTS CONTRIBUTE TO RESEARCH

Flatiron is committed to improve and extend lives by learning from the experience of every person with cancer.

In service of this mission, Flatiron works with a network of oncology clinics, several academic centers, the Food & Drug Administration, the National Cancer Institute, and biopharma companies, to create datasets that enable our clinics to provide the best care possible and researchers to accelerate their understanding of the way cancer treatments work. You can see some examples of how we're working to advance cancer research here.

For many oncology clinics across the country, Flatiron provides an electronic health record (EHR) software called OncoEMR®. If you are treated at one of these clinics, Flatiron accesses your data to help the clinics with your care and to use in a de-identified and aggregated form for research purposes. Flatiron also has partnerships with academic medical centers to provide quality monitoring and outcomes research.

As part of its engagements with oncology clinics and academic medical centers, Flatiron may also have certain additional rights pertaining to research and de-identification. Specifically, Flatiron has the ability to create de-identified datasets that are made available to third parties through Flatiron's real world data products. These products include tumor-specific and pan-tumor datasets with deep clinical, genomic and outcomes variables that may be used for research purposes by Flatiron's partners. The datasets we share with third parties for research purposes are de-identified in accordance with the expert determination method in accordance with the Health Insurance Portability and Accountability Act ("HIPAA") and never contain your personally identifiable information.

In addition to the de-identified datasets referenced above, certain of our engagements with oncology clinics and academic medical centers allow for Flatiron to conduct internal research using your data. In the rare instances that research cannot be done using Flatiron's de-identified real world data products, all such research is done pursuant to a waiver of the Authorization requirement by an institutional review board or privacy board in accordance with the standards set forth under HIPAA. Please note that even in those instances where internal research is done pursuant to a waiver, only the minimum amount of data that is required for the research is used and all direct identifiers relating to an individual patient are removed, such as name and social security number.

Please know that Flatiron will never use your information — even in de-identified form — for marketing purposes or for any other financial exchange with a third party. Additionally, we commit to maintaining and using de-identified data in a de-identified form and will not attempt to re-identify the information, except as permitted by law to determine if our de-identification processes are robust.

12. YOUR OPT-OUT RIGHTS

Your information, along with that of thousands of other patients, is contributing to cancer research and is helping to accelerate the development of new treatment options for future patients. However, we respect your right as a patient to opt-out of this research. If you wish to know whether you are treated at a clinic that uses Flatiron's technology, please ask your provider for the name of the EHR that they use. If you are still unsure whether your information is included in our datasets, or if you would like to opt-out of our research, please complete the online form. By filling out the online form, you give Flatiron permission to contact you to confirm any additional information needed to process your opt-out request.

Please be aware that your opt-out will apply only to Flatiron's future use of your Personal Information for research. Your opt-out will not apply to de-identified information that Flatiron US has already created for current and future research purposes. Further, your opt-out does not apply to certain practice-level OncoEMR reports or DataConnect files, which practices use for operational purposes, regulatory reporting, and other use cases. You should speak with your provider if you would like to be removed from any practice-initiated data projects.

13. CHANGES TO THIS NOTICE

We reserve the right to change or replace this Notice at any time. Please check back from time to time to ensure that you are aware of any changes or updates to the Privacy notice. We will indicate the date that the Notice was last updated at the top of this page. If we make material changes that would impact your use of the Sites or your privacy rights, we will endeavor to notify you of the changes, such as by posting a notice directly on the Sites or by sending an email notification if you have provided your email address to us.

14. CONTACT US

If you have any questions or comments about this Privacy Notice or for any privacy inquiries, including to exercise any of your privacy rights, please contact us at:

- Email: privacy@flatiron.com,
- Phone at 888-662-6367, or
- Mail: Flatiron Health, 233 Spring Street New York, NY 10013 US (Attn: Chief Compliance & Privacy Officer)