



Rush University System for Health

Privacy Notice for the General Data Protection Regulation (GDPR) (European Union)

This GDPR Privacy Notice (“Notice”) applies to people who reside in the European Economic Area (“EEA”) and demonstrates Rush University System for Health’s (“Rush”, “we”, “us” or “our”) commitment to comply with the European Union’s General Data Protection Regulation (“GDPR”). This Notice supplements the [HIPAA Notice of Privacy Practices of RUSH’s subsidiary hospitals](#).

Rush and its corporate affiliates, each in its own capacity, may act as a “Data Controller” under the GDPR. Rush’s primary place of business is located in the United States at 1725 W. Harrison St., Suite 364.

In this Privacy Notice, “you” means either yourself, if you are the patient, employee, student, contractor, or research subject in question, or may refer to your child or dependent, on whose behalf you are seeking that Rush offer medical treatment or employment, or permit research participation.

The GDPR requires Rush to provide you with certain information about your “Personal Data” as outlined in this Policy. This Notice describes how your Personal Data will be used by Rush and explains how Rush collects, uses and shares Personal Data gathered on subdomains and websites (“Sites”) through your use of Rush online services.

If you travel to the United States to receive treatment or receive educational services, you will receive a separate notice that describes how health care information or education records collected or generated in the United States will be treated by Rush.

1. What types of Personal Data does Rush collect?

Information you provide to Rush: You may provide Personal Information Data (as defined below) to Rush by receiving medical care at Rush, seeking employment at Rush, participating in a research study or clinical trial which Rush is involved, obtaining education at Rush, signing up for an online account through Rush, entering information through Rush’s online forms/surveys, or by contacting Rush via phone, email, or other communication portals.

Information from other sources: We may also obtain information about you from other sources and combine that information with information we collect from you directly. For example, we may collect information about you when you post content to our pages and/or feeds on third party social media platforms.

Categories of Personal Data generally collected by Rush include:

- Contact information, such as name, address, location, email, and telephone number.
- Online identifiers and other technical information, such as IP address, cookies, and username.
- Professional, employment, or education information.
- Financial information, such as insurance or credit card data for online payments.
- Education information, such as grade history, disciplinary actions, or other education related records;
- Health information related to medical history or records, treatment information, test results and medications. This may include information about your genetic information, HIV/AIDS status,



tuberculosis status, substance use disorders, mental health disorders, race, ethnicity, religious beliefs, gender identity and sexual orientation. Please also refer to the [HIPAA Notice of Privacy Practices](#) for [Rush University Medical Center \(RUMC\)/Rush Oak Park Hospital \(ROPH\)](#) and for [Rush Copley Medical Center \(RCMC\)](#) for more information.

- Research study participant qualification information, such as demographic and medical information used to determine whether you meet the eligibility criteria for enrollment into research studies; and
- Any other information that you provide to us that can be used to identify you.

We collect Personal Data about you in the following ways:

- When you submit information voluntarily. There are certain areas of the Sites where you can voluntarily submit Personal Data to Rush, such as when you register for an event, apply for a fellowship, or otherwise contact us directly;
- Through data collection technology. We use cookies and other data collection technology to collect and store your Personal Data when you interact with the Sites;
- Through social media, such as if you link to social media platforms or use social media plug-ins, we may (depending on your user privacy settings on that social media platform) automatically receive information about you from that social media platform; and
- From third parties, such as your health care providers, our marketing and bill payment partners, former employers, and publicly available sources.

In addition to Personal Data, we may collect other information that alone cannot be generally used to identify you. For example, when you use the Sites, we may collect your browser type, device type, and operating system information. If any of this information can be used to identify you because, for example, we link it to your Personal Data, we will treat such information as Personal Data.

2. How will Rush use your Personal Data?

The chart below describes the Personal Data that we collect, the likely sources of the Personal Data, how we may use and disclose it, for what purposes, and pursuant to what legal basis under the GDPR. Please also refer to the [HIPAA Notice of Privacy Practices](#) for [Rush University Medical Center \(RUMC\)/Rush Oak Park Hospital \(ROPH\)](#) and for [Rush Copley Medical Center \(RCMC\)](#) for more information for how we use and disclose Protection Health Information to provide health care items and services and conduct other activities subject to HIPAA.

Use of your Personal Data	Categories of Personal Data We Process	Source	Legal Basis under GDPR
Communications and Marketing			
Obtain your subscription preferences and	Contact information and other information you provide, such as your topic	You	<i>Legitimate interest:</i> To provide you with information you request or that we think might be of interest to you <i>Consent:</i> As required by law

Use of your Personal Data	Categories of Personal Data We Process	Source	Legal Basis under GDPR
send marketing communications	preferences and areas of interest		
Contact you regarding important administrative announcements	Contact information	You	<i>Legitimate interest:</i> To provide you with important information about the Services or the company, or our services
Respond to inquiries and fulfill requests	Contact information and other information you provide, such as your requests	You	<i>Legitimate interest:</i> To provide you with information you need and other services you request and to efficiently communicate with you
Conduct questionnaires and surveys	Contact information and other information you provide, such as your survey answers	You	<i>Legitimate interest:</i> To evaluate and take action with regard to your feedback and comments related to Rush
Register you for events and deliver event-related materials	Contact information and other information you provide, such as your preferences for the event	You	<i>Legitimate interest:</i> To enable your attendance at our events and to deliver you event materials <i>Contract:</i> As may be described on the registration page for the event
Perform website analytics and develop and improve our features, content, and services	Technical information and other information we collect, such as demographics, behavior, and event tracking	First and third party analytics cookies	<i>Legitimate interest:</i> To understand more about our visitors (what pages you view, how long you visit, your devices, etc.) in order to improve our services
Deliver advertising	Technical information and other information we collect, such as demographics, behavior, and event tracking	First and third party analytics cookies	<i>Legitimate interest:</i> To deliver advertising that is relevant to your preferences and demographics in an effort to improve your experience
Administration and Internal Operations			
Verify your identity	Contact information, other demographic information, and	You	<i>Legitimate interest:</i> To provide you with access to your account and information, and to prevent fraud

Use of your Personal Data	Categories of Personal Data We Process	Source	Legal Basis under GDPR
	Protected Health Information		
Provide access to the MyRush, MyChart, and other portals	Contact information, Protected Health Information, and other information about your demographics	You	<i>Legitimate interest:</i> To provide you with access to your account and offer portal-related services
Process your purchases, donations and other transactions	Contact information, financial information, and other information you provide when you donate, make a purchase or conduct a transaction	You	<i>Contract:</i> To process your purchase, donation or other transaction in accordance with your instructions.
Recruit personnel for employment, fellowship and training opportunities	Contact information, recruitment information, education and training information, and other information relevant to potential recruitment by Rush, such as employment records, criminal records, and demographics.	You, your references, your former employers, and publicly available sources, such as LinkedIn	<p><i>Pre-hire Measures:</i> To recruit and evaluate potential candidates to join Rush</p> <p><i>Legal obligations:</i> To comply with applicable legal obligations, including for employment law purposes</p> <p><i>Legitimate interest:</i> To make the best recruitment decisions for Rush</p> <p><i>Consent:</i> As required by law</p>
Medical Treatment and Clinical Research			
Schedule an appointment	Contact information, Protected Health Information, and other information necessary to schedule the appointment	You	<p><i>Consent:</i> As required by law</p> <p><i>Contract:</i> To provide the services you request</p> <p><i>Legitimate interest:</i> To schedule appointments for services that you request</p>
Locate a physician	Contact information and other information necessary to fulfill your request	You	<p><i>Legitimate interest:</i> To suggest a physician that would suit your needs</p> <p><i>Consent:</i> As required by law</p>
Evaluate your medical	Protected Health Information and other	You and your health	<i>Consent:</i> As required by law

Use of your Personal Data	Categories of Personal Data We Process	Source	Legal Basis under GDPR
condition(s) and provide you treatment	information necessary for your treatment.	care provider(s)	<p><i>Contract:</i> To provide the treatment that you request</p> <p><i>Legitimate interest:</i> To provide the treatment that is medically appropriate for the patient and as permitted by HIPAA or other applicable law and the HIPAA Notice of Privacy Practices</p>
Review requests to participate in research studies and screen eligibility for enrollment	Contact information, research study participant qualification information, and other information relevant to your eligibility and qualifications to participate in research studies at Rush.	You and your health care provider(s)	<p><i>Consent:</i> As required by law</p> <p><i>Scientific and research purposes:</i> To engage in clinical research in accordance with applicable laws and regulations</p> <p><i>Legal obligations:</i> To comply with applicable legal obligations</p> <p><i>Legitimate interest:</i> To ensure research subjects are eligible and appropriate for the studies</p>

We may also aggregate or anonymize your Personal Data so that it can no longer be used to identify you. This aggregate or anonymize information may be used for any purpose permitted by law.

Other Uses: In the event of any other purposes for which we wish to use your Personal Data that are not listed above, or any other changes we propose to make to the existing purposes, we will notify you by amending this Notice as provided herein.

3. How will Rush share my Personal Data?

We will share your Personal Data within Rush, at your direction, as disclosed to you at the time of collection, or in the following circumstances:

- Service Providers:** We may provide your Personal Data to our services providers that help us run and manage our organization and process Personal Data solely on our behalf. The categories of service providers include, but are not limited to, electronic medical record vendors, data analytics, information technology and cloud services, auditing and consulting firms, clinical research organizations, laboratories, marketing companies, payroll and benefit companies, and telehealth providers.
- Corporate Transaction:** In the event Rush is involved in a merger, reorganization, acquisition or sale of all or a portion of its assets, or other corporate transaction such as a joint venture, we may disclose your Personal Data as part of that transaction.



- **As Required By Law:** We may disclose your Personal Data if we determine that the disclosure is necessary: (i) to comply with any law applicable to us, a request from law enforcement, a regulatory agency, or other legal process; (ii) to protect the legitimate rights, privacy, property, interests or safety of Rush, our business partners, personnel, or the general public; (iii) to pursue available remedies or limit damages; (iv) to enforce applicable policies or procedures; or (v) to respond to an emergency.

We reserve the right to disclose or sell non-identifiable aggregate or anonymized information to third parties for any lawful purpose.

4. Retention

We will keep your Personal Data for as long as necessary to fulfill the purposes for which we collected it, including any legal, professional, accounting or reporting requirements and in accordance with our internal policies. To determine the appropriate retention period, we consider the amount, nature, and sensitivity of Personal Data, the potential risk of harm from unauthorized use or disclosure of your Personal Data, the purposes for which we process your Personal Data, whether we can achieve those purposes through other means, and all applicable legal requirements.

5. International Transfer of Personal Data

Rush is committed to complying with this Notice and data protection laws, including those outside of the United States, that apply to our collection and use of your Personal Data. Rush is located in the United States, and we recognize that the laws in the United States may be different and, in some cases, not as protective as the laws other countries, including those located in the EEA. By providing us with your Personal Data and using our Sites, you acknowledge that your Personal Data will be transferred and processed in the United States. If you would like to know more about how we protect your Personal Data, you can contact us using the information in the section “Contact Us” at the end of this Notice.

6. Security

We seek to use reasonable physical, technical, and administrative measures designed to protect Personal Data within our organization. Unfortunately, no data transmission or storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of your account has been compromised), please immediately notify us in accordance with the “Contact Us” section below.

7. Your Rights:

If you are located in the EEA and we maintain your Personal Data, you may have the following rights (under the GDPR) with respect to your Personal Data that is held by Rush. In particular, you may have the right to:

- **Right to access and receive:** You may request a copy of or access to the Personal Data we hold about you. You may also request that we transfer your Personal Data to a third party in a machine-readable format.



- **Right to correct:** You may ask us to update or correct inaccurate or incomplete Personal Data we hold about you.
- **Right to limit or restrict:** You may have the right to request that we stop using all or some of your Personal Data or to limit our use of it.
- **Right to erase:** You may have the right to request that we delete all or some of your Personal Data. This right may be limited if we have collected your Personal Data for research purposes.
- **Right to withdraw consent:** You have the right to withdraw any consent you have previously given to Rush at any time. Your withdrawal of consent does not affect the lawfulness of our collecting, using, and sharing of your Personal Data prior to the withdrawal of your consent. Even if you withdraw your consent, we have the right to use your Personal Data if it has been fully anonymized and cannot be used to personally identify you.

These rights may be limited in certain ways, including if your Personal Data is required for Rush to perform a contract, protect its rights and interests or those of a third party, to defend against a legal claim, or to comply with applicable laws or regulations.

You are also entitled to file a complaint with your national or local data protection authority. You may find a list of such authorities at the following web page: http://ec.europa.eu/jusitce/data-protection/articla-29/structure/data-protection-authorities/index_en.htm.

To exercise any of these rights, please contact Rush at the information contained at the bottom of this Notice. We will respond to your inquiry within a reasonable timeframe and may charge a small fee if your requests are manifestly unfounded or excessive.

If you wish to exercise any of your rights (including the rights of individuals in the European Economic Area discussed below), please contact us using the information in the “Contact Us” section at the end of this Notice. If we are unable to honor your request, or before we charge a fee, we will let you know why.

Please note that if you decide to exercise some of your rights, we may be unable to provide you certain services, or you may not be able to use or take full advantage of the services we offer.

8. Cookie Policy

Our sponsors and advertises and their ad servers may use cookies when you view pages on our Site(s). They use those cookies to collect information as a way of measuring the effectiveness of their advertising, or to provide advertisements about goods and services that may be of interest to you or to avoid running the same ads to you over time. Such information may include your browser type, your operating system, web pages visited, time of visits, content viewed, ads viewed and other clickstream data. For more details about cookies, please see our [Cookie Notice](#).

9. Children’s Privacy

The Sites are neither directed at individuals under the age of 16, nor does Rush knowingly collect Personal Data from children under 16 without parental consent, except where necessary to protect the vital interests of the child, and except in accordance with Illinois law. If Rush becomes aware that a child under 16 has provided Rush with Personal Data on our Sites improperly, Rush will take steps to delete such information, when necessary. If you become aware that a child has improperly provided Rush with



Personal Data on our Sites, please contact the Privacy Office at Rush University Medical Center (phone: (312) 942-5303 or privacy_office@rush.edu) or Rush Copley Medical Center (phone: 630-499-4721)

10. Whom do I contact with questions about my Personal Data or Processing activities?

If you have questions about the processing of your Personal Data or to exercise the rights discussed in this Notice, contact the Data Protection Officer, Rush University Medical Center (312-942-5303, privacy_office@rush.edu) or the Privacy Office at Rush Copley Medical Center (630-499-4721)

For more information about how Rush collects and processes protected health information (PHI) in the United States to provide healthcare and education services, please refer to the appropriate Rush entity's [HIPAA Notice of Privacy Practices](#) for [Rush University Medical Center \(RUMC\)/Rush Oak Park Hospital \(ROPH\)](#); [Rush Copley Medical Center \(RCMC\)](#); and Rush University [FERPA Notice](#) for more information.

Note, policy changes may occur at any time to any policy. Rush encourages you to periodically review our policies to ensure you are familiar with the most current version.