MyHSS General Data Protection Regulation Privacy Disclosures

Effective Date: May 25, 2018
Last Updated: May 25, 2018

The following GDPR privacy disclosures (the **Disclosures**) describe how HSS and our affiliates, including, but not limited to HSS' related entities, (collectively, **us**, **we** or **HSS**) collect, use and share the Personal Information of individuals located in the European Union, Iceland, Liechtenstein, or Norway (the **European Economic Area** or **EEA**) when such actions are within the scope of the European Union's General Data Protection Regulation (**GDPR**) (collectively, the **EEA Processing Activities**). These Disclosures apply to Personal Information gathered by electronic means through HSS' patient portal, MyHSS (the **Services**).

If you would like additional information about the ways HSS may collect, use and share information that can be used to directly or indirectly identify you, please click here.

HSS is the controller of the Personal Information described below.

If you have any questions about the Disclosures or our information practices, please contact us using the options provided below.

THE DISCLOSURES APPLY ONLY TO THE USE OF PERSONAL INFORMATION IN EEA PROCESSING ACTIVITIES

How We Collect and Use Personal Information

When we use the term **Personal Information**, we mean information that can be used to identify you as an individual person, either directly or indirectly. We collect several categories of Personal Information through our Services, including information you provide, information collected automatically (potentially including location information), and information we obtain from third party sources.

We generally use the Personal Information we collect to operate the various functions of HSS and provide the HSS services that may be available to you.

We rely on separate and overlapping bases to process your Personal Information lawfully. By way of example only, it may be necessary for us to process your Personal Information in certain ways in order to process a transaction you requested or otherwise in accordance with a contract between us, or in certain cases we may process your Personal Information as necessary to conduct HSS' legitimate interests, when those legitimate interests are not overridden by your rights and interests.

The ways in which we collect and use your Personal Information vary depending on the relationship between you and HSS, as well as the specific HSS function with which you interact. The following Disclosures are intended to describe, in more detail, our collection and use practices related to your use of the MyHSS patient portal.

MyHSS

HSS and its affiliates may collect certain information to facilitate your treatment at HSS and to process transactions requested by you. **When you first present for care at HSS in the United States, you will generally be provided a separate Notice of Privacy Practices that explains in more detail the types of data collected and the purposes for which such data are processed and shared by HSS. That Notice will control regarding the data collected during the course of your treatment at HSS; these Disclosures apply to information that you provide while located in the EEA.** If you have additional questions about the processing of your data in connection with your becoming or being a patient at HSS, please contact us using the options provided below.

Category of Personal Information	*Purposes of Processing*	*Legal Bases for Processing*
Contact Information including your name, home address, email address and phone number	To notify you of upcoming appointments, process payments, and maintain health records	To process transactions requested by you and meet our contractual obligations Legitimate interests Your consent, if applicable
Health Records including doctor's records, surgical records, immunizations, medications, genetic testing information, and biometric information	To treat you	To process transactions requested by you and meet our contractual obligations Legitimate interests To protect your vital interests Your consent, if applicable For diagnosis and treatment
Family Information including family members, ages, occupations, and health	To treat you and maintain accurate health records	To process transactions requested by you and meet our contractual obligations Legitimate interests To protect your vital interests Your consent, if applicable For diagnosis and treatment
Employment History including prior employers, titles, wages, work experience, trade union membership, and disciplinary record	To process insurance coverage and payment for treatment	To process transactions requested by you and meet our contractual obligations Legitimate interests Your consent, if applicable For diagnosis and treatment
Demographic Information including race, ethnicity, gender, age, education,	To treat you and maintain accurate health records	To process transactions requested by you and meet our contractual obligations

profession, occupation, income level, and marital status		Legitimate interests Your consent, if applicable For diagnosis and treatment
Payment Information including the last 4 digits and expiration date of your payment card	To process your payment for services rendered	To process transactions requested by you and meet our contractual obligations Legitimate interests Your consent, if applicable
Log Files including IP addresses, browser type, internet service provider, referring/exit pages, operating system, date/time stamp and/or clickstream data	To notify you of upcoming appointments, process payments, and maintain health records	To process transactions requested by you and meet our contractual obligations Legitimate interests Your consent, if applicable
Location Information We may use your IP address to identify the general geographic area from which you are accessing hss.edu	To conduct analytics to improve the Services, track user trends, and create custom audience lists We collect data from different systems but do not link IP addresses to any Personal Information	Legitimate interests Your consent, if applicable

Information We Obtain from Third Party Sources

We may obtain certain Personal Information about you from third party sources, which we may use to serve our legitimate interests, comply with legal obligations, perform a contract, or in some cases, in accordance with your consent.

Partners and Service Providers

We use partners and service providers, such as payment processors and analytics providers, to perform services on our behalf. Some of these partners have access to Personal Information about you that we may not otherwise have (for example, if you sign up directly with that provider) and may share some or all this information with us. We use this information to administer the Services and to process transactions that you request.

Supplemental Information

We may receive additional Personal Information from third-party sources, such as credit reference agencies and public databases, which we may append to existing Personal Information, such as email address verification. We may use this supplemental information to process transactions that you request and to prevent fraud, deliver relevant offers and advertising to you and to improve our operations and Services.

Additional Uses of Personal Information

In addition to the uses described above, including, but not limited to, under "Purposes of Processing" and "Information We Obtain from Third Party Sources," we may use your Personal Information for the following purposes, which uses may under certain circumstances be based on your consent, may be necessary to fulfill our contractual commitments to you, and are necessary to serve our legitimate interest in the following operations:

- Conducting our operations, administering the Services and managing your accounts;
- Contacting you to respond to your requests or inquiries;
- Processing and completing your transactions including, as applicable, processing online payments, and delivering products or services;
- Providing you with newsletters, articles, service alerts or announcements, event invitations, and other information that we believe may be of interest to you;
- Providing you with promotional information, offers, and other information that are personally tailored to your interests;
- Conducting market research, surveys, and similar inquiries to help us understand trends and needs of our users;
- Alerting you about a safety announcement;
- Preventing, investigating, or providing notice of fraud, unlawful or criminal activity, or unauthorized access to or use of Personal Information, our website or data systems; or to meet legal obligations; and
- Sending you text messages or push notifications when you sign up for one of our messaging programs. These messages may be sent by automated means.

Legitimate Interests

We rely on several legitimate interests in using and sharing your Personal Information. These interests include:

- improving and customizing the Services for you;
- understanding how the Services are being used;
- obtaining insights into usage patterns of the Services;
- exploring ways to develop and grow our operations;
- ensuring the safety and security of the Services;
- conducting research and improving understanding in fields of public interest and health; and
- enhancing protection against fraud, spam, harassment, intellectual property infringement, crime and security risks.

Data Retention

We will retain your Personal Information only for as long as is necessary for the purposes set out in the Disclosures, subject to your right, under certain circumstances, to have certain of your Personal Information erased (see **Your Rights** below), unless a longer period is required under applicable law or is needed to resolve disputes or protect our legal rights.

How We Share and Disclose Personal Information

We share your Personal Information with third parties only in the ways described in the Disclosures. We may share your Personal Information within HSS, with HSS' affiliates, service

providers and partners, and to comply with the law, protect health and safety and enforce our legal rights.

Service Providers

We share your Personal Information with third-party service providers who complete transactions or perform services on our behalf or for your benefit, such as:

- Coordination of care
- Payment and donation processing
- Marketing and analytics
- Event registration and coordination
- Course registration and coordination

Affiliates

We may share your Personal Information within HSS and with our affiliates for purposes and uses that are consistent with the Disclosures.

Partners

We may share your Personal Information with our partners for the purposes of administering programs and services.

Third-Party Mobile App Providers

With your knowledge and consent, the Services may gather and transfer your Personal Information, including location information, from and to other applications, functions and tools within your mobile device.

Social Media Platforms

We may also use services provided by third parties (such as social media platforms) to serve targeted ads to you on third party platforms. We may do this by providing a hashed version of your Personal Information to the third party for matching purposes. For more information, including on how to control your privacy settings and your ad choices, read our Cookie Policy.

Legal Process, Safety and Terms Enforcement

We may disclose your Personal Information to legal or government regulatory authorities, as required by applicable law. We may also disclose your Personal Information to third parties as required by applicable law in connection with claims, disputes or litigation, when otherwise required by applicable law, or if we determine its disclosure is necessary to protect the health and safety of you or us, or to enforce our legal rights or contractual commitments that you have made.

International Data Transfers

HSS may transfer your Personal Information within HSS, to HSS' affiliates, and/or to the third parties discussed above. Your Personal Information may be transferred to, stored, and processed in a country other than the one in which it was collected.

If your Personal Information was collected or stored in the EEA, we may transfer your Personal Information outside the EEA and when we do so, we rely on appropriate or suitable safeguards recognized under data protection laws.

Adequacy Decision

We may transfer your Personal Information to Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the United States (limited to those transfers governed by the EU-U.S. Privacy Shield framework), and any other countries that the European Commission has approved as providing adequate protection to Personal Information.

Standard Contractual Clauses

The European Commission has adopted standard data protection clauses, which provide safeguards for Personal Information transferred outside of the EEA. We may use Standard Contractual Clauses when transferring Personal Information from a country in the EEA to a country outside the EEA. You can request a copy of our Standard Contractual Clauses by contacting us as set forth in the **Contact Us** section below.

With Your Consent

In respect of certain cross-border personal data transfers, we will obtain your consent to transfer your Personal Information outside the EEA after first informing you about the possible risks of such a transfer.

By Contract

We will transfer your Personal Information outside the EEA if the transfer is necessary to the performance of a contract between you and HSS, including to provide treatment to you, or if the transfer is necessary to the performance of a contract between HSS and a third party, such as your physician or other health care provider located in the EEA, and the contract was entered into in your interest.

Additional Considerations

In addition, we may transfer your Personal Information outside the EEA if the transfer is necessary to establish, exercise or defend legal claims or to protect your vital interests.

Children

Protecting the privacy of children is very important to HSS. Thus, we do not collect or maintain Personal Information, from anyone we know to be under age 13.

Your Rights

We process all Personal Information in compliance with your rights, in each case to the extent required by, and in accordance with, applicable law (including any applicable time limits and fee requirements).

General Data Protection Regulation (GDPR)-Specific Rights

These rights apply only to Personal Information collected during EEA Processing Activities. Upon request, we will provide you with information about whether we hold any

of your Personal Information, along with any details required to be provided to you under applicable law. In certain cases, you may also have a right to:

- amend any of your Personal Information that is inaccurate;
- to restrict or limit the ways in which we use your Personal Information;
- to object to the processing of your Personal Information;
- to request the deletion of your Personal Information, and
- to obtain a copy of your Personal Information in an easily accessible format.

To submit a request, please contact us as set forth in the **Contact Us** section below. We will respond to your request within a reasonable time.

You also have the right to withdraw your consent to our processing of your Personal Information, if our processing is solely based on your consent. You can do this by discontinuing use of the Services, including by closing all your online accounts with us and contacting us as set forth in the **Contact Us** section below to request that your Personal Information be deleted. If you withdraw your consent to the use or sharing of your Personal Information for the purposes set out in the Disclosures, you may not have access to all (or any) of the Services, and we might not be able to provide you all (or any) of the Services. Please note that, in certain cases, we may continue to process your Personal Information after you have withdrawn consent and requested that we delete your Personal Information, if we have a legal basis to do so. For example, we may retain certain information if we need to do so to comply with an independent legal obligation, or if it is necessary to do so to pursue our legitimate interest in keeping the Services safe and secure, or if deleting the information would undermine the integrity of a research study in which you are enrolled.

If you have any complaints regarding our privacy practices, you have the right to lodge a complaint with your national data protection authority (i.e., supervisory authority).

Links to Third Party Sites

The Services may include links to websites and digital services operated by third parties. The Disclosures do not apply to, and we are not responsible for the content, privacy policies or data practices of, third parties that collect your information. We encourage you to review the privacy policies for those third parties to learn about their information practices.

The Services may feature widgets hosted by other companies. These features may collect your IP address, which page you are visiting on our Services and may set a cookie to enable the feature to function properly. The loading, functionality and your use of the plugins are governed by the privacy policy and terms of the third party that provided the plugin.

User Generated Content

Some of our Services may enable users to submit their own content. Unless otherwise indicated, please remember that any information you submit or post as user-generated content to the Services become public information. You should exercise caution when deciding to disclose your personal, financial or other information in such submissions or posts. We cannot prevent others from using such information in a manner that may violate the Disclosures, the law, or your personal privacy and safety. We are not responsible for the results of such postings.

Updates to the Disclosures

The Disclosures are subject to occasional revision, and if we make any material changes in the way we use your Personal Information, we will notify you by sending you an email to the last email address you provided to us and/or by prominently posting notice of the changes on the Services and updating the effective date above.

Any changes to the Disclosures will be effective upon the earlier of 30 calendar days following our dispatch of an email notice to you, or 30 calendar days following our posting of notice of the changes on the Services. These changes will be effective immediately for new users of our Services.

You are responsible for updating your Personal Information to provide us with your most current email address. If the last email address that you have provided us is not valid, or for any reason is not capable of delivering to you the notice described above, our dispatch of the email containing such notice will nonetheless constitute effective notice of the changes described in the notice.

If you do not wish to permit changes in our use of your Personal Information, you must so notify us prior to the effective date of the changes and discontinue using the Services. Continued use of our Services, following notice of such changes shall indicate your acknowledgement of such changes and agreement to be bound by the terms and conditions of such changes.

Managing Communication Preferences

If you have opted in to our marketing (or when permitted by law, if you have provided us with your contact information), we may send you email messages, direct mail, push notifications or other communications regarding products or services, depending on the method of communication selected. You may ask us not to do so when you access our websites or mobile applications, or change your preferences by updating any accounts you have with us. At any time, you may elect to discontinue receiving messages about these products or services from us by submitting an opt-out request to the contact information below, or by following the unsubscribe instructions in the form of the communication you received, as described below.

Printed Materials

To opt out of receiving printed materials about our products or services at your postal address, please write to us at the address set forth in the **Contact Us** section below. Please be sure to include your name, mailing address and description of the marketing material received exactly as they appear on the printed marketing materials you received.

Emails

To opt out of receiving communications about our products or services via email, please send an unsubscribe request to the email address set forth in the **Contact Us** section below or click on the unsubscribe link at the bottom of the email that was sent to you and follow the directions on the resulting web page. Please note that you may continue to receive certain transactional or account-related electronic messages from us.

Text Messages

If you have consented to receive text messages, you may opt out of receiving them by using the method provided in the text message or by contacting us as set forth in the **Contact Us** section below.

Push Notifications

To opt out of receiving push notifications, please set your preferences within your device setting menu.

Contact Us

If you have any questions, comments, requests or concerns about the Disclosures or other privacy-related matters, you may contact us in the following ways:

Email:	GDPR-Inquiry@hss.edu
Phone:	212-774-7500
Address:	535 East 70th Street New York, NY 10021

For purposes of the General Data Protection Regulation:

Representative:	VP, Corporate Compliance & Internal Audit Hospital for Special Surgery 535 East 70th Street New York, NY 10021 212-774-7500
Data Protection Officer:	Chief Information Security Officer Hospital for Special Surgery 535 East 70th Street New York, NY 10021