Website Privacy Policy

Note: This policy relates specifically to our website. For HIPAA Notice of Privacy Practices, please see above.

WE RESPECT YOUR PRIVACY. THIS PRIVACY POLICY DESCRIBES HOW WE COLLECT AND USE YOUR PERSONAL INFORMATION. PLEASE READ IT CAREFULLY.

The websites and services provided through the website are provided by Hospital Sisters Health System and its affiliates. You have a limited right to access and use the site for your noncommercial, personal use and information only.

What Information Do We Collect?

Information that you provide to us. For example, you provide information when you:

- Fill out forms on the site
- Provide information to open an account
- Communicate with us by social media, email, or chat
- Respond to surveys.

Some areas of the site are available without opening an account. Other areas of the site cannot be accessed without registering, which requires you to provide personal information to us for personalization and verification.

This personal information may include your:

- Name
- Address (including city, state, and ZIP code)
- Phone number
- Email address
- Information pertaining to your health
- Information related to your employment
- Information related to your affiliation with us
- Age
- Gender
- Preferences, interests, and favorites.
- In addition, we collect information about your visit to the site.

For example, we may collect:

- Information about the network you use to access the Internet, including, but not limited to, domain and hosting information.
- Information about the device you are using, including, but not limited to, location, browser, screen resolution, and operating system.
- Information about your visit to our site, including, but not limited to, which pages you visited, amount of time on site, traffic sources, site search usage, and actions taken.

Tracking Technologies

We only use tracking technologies to retrieve information from your device for purposes related to our site or your interaction with our site.

Cookies

“Cookies” are small text files stored on your device that help us remember your preferences. We primarily use cookies that are considered 'mandatory' or 'technically necessary' to provide our site and its core functionality to you (e.g., cookies that store your log-in information or remember other settings, so you don't have to re-enter them each time you return to our site).

Scripts

Tracking scripts are code snippets that collect information about how you interact with our site. We primarily use tracking scripts to obtain high-level "audience measurement" data such as traffic sources, type of operating system and browser used, date, time and length of visit, and other information related to user behavior on our site for the purpose of understanding and optimizing the site experience. To ensure tracking script data cannot be linked back to an identifiable user, all IP Addresses collected are anonymized and Business Associate Agreements have been signed with all third-party service providers.

Disabling Tracking Technologies
You may stop or restrict tracking technologies (including cookies and scripts) on your device or purge them from your browser by adjusting your web browser preferences. You should consult the operating instructions that apply to our browser for instructions should you wish to do so and in general to determine how best to configure your browser settings to meet your requirements. Most browsers also offer controls for third-party scripts through privacy settings or extensions.

Note: if you "turn off," purge, disable cookies, or block scripts, although you may still use our site, you may not be able to use all the features, functions, or services available on our site.

How We Use Information

We do not sell or license your information. We use the information you provide, and we collect to:

- Operate the site
- Provide the services you request.
- Administer the site and diagnose problems with our technology and platforms;
- Verify your identity;
- Provide you with information about the site;
- Assist you and help us perform responsibilities described in the Terms of Use;
- Monitor user behavior and analyze patterns to personalize and optimize the site experience for you;
- Deliver relevant content to you;
- Provide authorities or relevant individuals with information related to the site as required by law; and
- Fulfill any other purpose for which you provide information.

These are the limited ways we interact with your information in connection with our mobile applications:

- When you choose to add a profile photo to our mobile applications, you may select an existing photo on your device or take a new photo using the camera app on your device. If you select an existing photo on your device, we store a copy of your chosen photo in app-private storage on your device. If you use the camera app on your device to take a new photo, the photo you take is first saved to your camera app and then also saved to app-private storage on your device. If you remove the photo from your profile or delete our mobile apps, the copy of the photo is deleted from the app-private storage, but the photo saved to your camera app remains available in your camera app until you choose to delete it. If you already have a photo stored in your profile through your health care organization – we do not interact with that photo in any way.
- When you choose to use Apple's HealthKit or Google Fit, we create encrypted identifiers to identify recipients of your Apple's HealthKit or Google Fit data and store them on your device in app-private storage. If you choose to stop using Apple HealthKit or Google Fit or delete our mobile apps, the identifiers are deleted.
- When you choose to view documents from your health care organization (such as letters or images) using our mobile apps, to make the files viewable for you we temporarily store copies on your device in app-private storage. The temporary copies are deleted when you close your session on our mobile apps.
- If your health care organization offers automatic appointment arrival and you choose to enable it, we temporarily store identifiers and times for your upcoming appointments in app-private storage to detect when you arrive for an upcoming appointment. If you stop using our mobile apps or disable automatic appointment arrival, the identifiers are deleted.
- If your health care organization offers location-based check in for in-person appointments or allows you to find health care providers near you, you may choose to allow our mobile apps to interact with your location data for those purposes. We do not store your location data.

- If your health care organization allows you to notify front desk staff electronically when you arrive for an appointment, you may choose to allow our mobile apps to interact with your Bluetooth data for this purpose. We do not store your Bluetooth data.
- While you use our apps, we collect non-identifying information so we can provide customer service to you or your health care organization and understand how people use our mobile apps so we can improve our products. This information includes the time you began using the app, the health care organization you interacted with, any error messages or codes, the model of device used and its operating system, and the version of our mobile app used. If you use Android devices, we also collect your connection type (cellular or Wi-Fi) during an error.
- You may contact us through the methods listed on our website. If you contact us, we may keep a record of the communication. You can decide how much information you want to share with us in those cases.

Your Health Care Organizations
To use our mobile apps, you must have an account with a health care organization using Epic's software. Because of this, your use of our mobile apps is also subject to your health care organization's privacy policy. Please contact your health care organization if you have any questions about their privacy policy.

How We Share Information

We do not use or disclose sensitive personal information, such as race, religion, or political affiliations, without your express consent. We expect that all collection, use and disclosure of your information will occur in the United States and will be governed by United States law; however, some information may travel over the internet outside of the United States. Even if some information does travel outside the United States, you agree that the laws of the United States will apply.

We will not sell or rent your information to anyone, but we may share your basic demographic information (such as your name, location, and physical or email address) with others, such as our subsidiaries, contractors, trusted partners, and affiliates as necessary to operate our business, and as permitted by law. If we share data with trusted partners in support of the programs, services, and content we provide, such third parties are prohibited from using your personal information except to provide these services to us, and they are required to maintain the confidentiality of your information. We do not share your personal information with third parties for their direct marketing purposes.

What About Aggregated Data?

We may aggregate (combine) data about visitors to our site in a non-identifiable manner and use it for our business purposes unrelated to your use of the site. For example, we may aggregate data for product development and improvement activities and disclose such aggregated data to third parties.

What about Governmental and Legal Disclosures?

Except as described above, we do not disclose the identities of visitors or users of the site unless legally required to do so, or unless we believe, in good faith, that sharing is necessary:

- to protect your safety or the safety of others,
- to protect our rights,
- to investigate criminal activity, or
- to respond to a government request.

We will respond to any subpoena received from a government agency without prior notice to you. Unless prohibited by law or by a valid court order, we will attempt to notify you of any subpoena received from any other party which requires us to disclose your identity, and will wait ten (10) days, or a lesser amount of time as required by the deadline in the subpoena, before providing the information requested by the subpoena.

What about Other Information and Websites?

Some content or applications on the site may be served by third parties. These third parties may use tracking technologies to collect information about you when you use our site. The information they collect may be associated with your personal information or they may collect information, including personal information, about your online

activities over time and across different websites and other online services. They may use this information to provide you with interest-based (behavioral) advertising or other targeted content.

We do not control these third parties' tracking technologies or how they may be used. You should review the privacy policies posted on these websites carefully before providing any information. We are not responsible for the privacy policies or the content of any other websites. If you have any questions about an advertisement or other targeted content, you should contact the responsible provider directly.

Do Not Track Signals

We may track your movement through the site and across third party websites to provide improved experiences and relevant content, and therefore we do not respond to Do Not Track (DNT) signals. However, some people do not want their browsing behavior to be tracked. Your web browser allows you to set the DNT signal on your browser so that third parties know you do not want to be tracked. We also suggest you read the privacy policies of third-party websites to see if those websites track your browsing.

COPPA

The site is not built for children under the age of 13. We comply with the Children's Online Privacy Protection Act ("COPPA") and do not knowingly permit registration or submission of personally identifiable information by anyone under 13 years of age. This age requirement is posted each time we request personally identifiable information. If you believe information about a child under 13 has been submitted, please advise us in writing and we will remove it.

International Privacy Laws

If you are visiting our websites from outside the United States, please be aware that you are sending information (including personal data) to the United States, where our servers are located. That information may then be transferred within the United States or back out of the United States to other countries.

All data collected through the site will be stored exclusively in secure hosting facilities provided by us or our service providers. We have data processing agreements in place with our service providers consistent with applicable privacy and data security laws.

Hospital Sisters Health System and its affiliates are located and provide services in the United States and are governed by United States law.

For visitors from the European Union, countries outside of the EU (such as the United States) may not necessarily have data protection laws as comprehensive or protective as those in your country of residence.

The United States has not been issued an adequacy decision finding the data privacy laws to provide an adequate level of protection, and no other basis for transfer exists. Therefore, the collection and transfer of data will occur on one of the following bases, depending on the type of transfer and the surrounding factual situation:

- The transfer is necessary for the performance of a contract between you and a Hospital Sisters Health System entity. This will apply when, for example, you are buying a product or signing up for information.
- The transfer is necessary for the conclusion or performance of a contract between Hospital Sisters Health System and another person or entity that is in your interest. This will apply when, for example, you request a product or further information from a third party through our site.
- The transfer is necessary for the establishment, exercise, or defense of legal claims. This would apply if there developed a dispute between you and a Hospital Sisters Health System entity.
- You explicitly consent to the transfer, having been informed of the possible risks of the transfer. Possible risks include:
    - While we exercise great care to protect personal data, it is possible that we may be required to produce personal data to U.S. legal authorities upon presentation of a subpoena, court order, search warrant, or other legal process. We will evaluate the legal process and resist such legal demands on your behalf unless it is clearly valid based on the legal opinion of our attorneys.

- The data protection laws in the United States may also provide for other uses of data, including uses for marketing that differ from the use for which the data was originally collected ("secondary uses"); however, except where otherwise compelled by law, our collection, storage, and use of your personal data will at all times continue to be governed by this Privacy Policy.

Site Security

The site has security measures in place to protect against the loss, misuse, or alteration of information under our control. However, no security is perfect, and no security system can prevent all security breaches. You transmit information to us at your own risk. You acknowledge that the site is not HIPAA compliant. You should not store or transmit Protected Health Information (PHI) on this site. You acknowledge and agree that the site is not intended to provide any medical advice. We are not your business associate under HIPAA because of your use of the site.

Amendments & Updates

We may update the Privacy Policy to reflect company policy changes, customer feedback, or legal requirements. We encourage you to periodically review the Privacy Policy to remain informed of how we use and protect your information. Our use of information gathered or obtained is subject to the Privacy Policy in effect at the time of such use.

Questions, Requests & Feedback

We welcome your comments regarding this Privacy Policy. If you have any questions or feedback regarding this Privacy Policy, please contact us at:

Hospital Sisters Health System
Attn: Privacy Officer
4936 Laverna Road
Springfield, Illinois 62794-9456
(217) 757-3258
PrivacyDepartment@HSHS.org

We will use reasonable efforts to promptly respond to your inquiry, and if necessary, determine and remedy any problem.

What If My Information is Wrong?
You may write to us at the contact address above if you believe the information you submitted to us through the site is incorrect. We may not be able to correct that information, because, for example, we did not save the information in question, or because we do not yet have a process to update the information.

Can I Get a Copy of My Information?
You may write to us at the contact address above to request a copy of the information you have submitted, or we have collected about you through the site. If we can collect and provide the information, we will do so. In some cases, we may not be able to collect and provide the information, because of the way the data is used and stored.