

WPS Website Privacy Policy

Eligibility

At Wisconsin Physicians Service Insurance Corporation (WPS), and/or its wholly owned subsidiary, The EPIC Life Insurance Company (hereinafter “WPS”), we take our customers’ privacy seriously and understand that visitors of our website need to be in control of their personally identifiable information (name, email address, postal address, etc.). This statement discloses the information practices for WPS and its wholly owned subsidiary, including what type of information is gathered and tracked, how that information is used, and with whom the information is shared.

Our Information Collection and Use Practices

Your information may be collected by WPS for internal marketing and development purposes. WPS will not sell any personal information to third parties for purposes of marketing, advertising, or promotion. WPS does, however, use cookies to track language preferences and Google Analytics as described later in this policy.

Data Collection, Use and Disclosure

WPS will not gather personally identifiable information about you unless you specifically and knowingly provide this information to us. Personally identifiable information (PII) is any information about an individual maintained by WPS with respect to, but not limited to, education, financial transactions, medical history, and criminal or employment information that can be used to distinguish or trace an individual’s identity (e.g., name, Social Security number, date and place of birth, mother’s maiden name, biometric etc.), including any other personal information linked or linkable to an individual.

Personal Information

WPS websites may include web pages that give you the opportunity to provide us with personal information about yourself. You do not have to provide us with personal information if you do not want to; however, that may limit your ability to use certain functions of this website or to request certain services or information.

You may choose to give us personal information in a variety of situations. For example, you may give us information, such as your name and address or email address, to correspond with you, or to sign up for our newsletter. Additionally, WPS may collect specific PII from you when you enroll in our customer, provider or employer portal(s) to establish your account and to properly authenticate you for access to the portal. **We intend to let you know how we will use such information before we collect it from you; if you tell us that you do not want us to use this information to make further contact with you beyond fulfilling your requests, we will respect your wishes.**

If you provide us with personally identifiable information, including your name and contact information (address, email, telephone number), we may use this information to contact you directly. If you give us personal information about somebody else, such as a spouse or work colleague, we will assume that you have their permission to do so.

Forms and Transactions

WPS sites may use online data entry forms to collect personal information from web visitors who choose to identify themselves for the purpose of transacting e-commerce or receiving products, services, or information.

For example, if you complete applications and forms or request something from the WPS site, such as a product or service, a callback, or specific marketing materials, we will use the information you provide to fulfill your request. Your information, including your personal information, may be shared with third parties, for instance, WPS Business Partners, to complete your transaction. In connection with a transaction, we may also contact you as part of our customer satisfaction surveys or for market research purposes.

Sharing Personal Information

WPS is committed to ensuring that our customers’ information is properly collected, used, and maintained. WPS and its wholly owned subsidiary may share your personal information with one another to support our business operation, to provide services to you, and for any other purpose described in this Privacy Policy.

We will not disclose, give, sell, or transfer any personally identifiable information that you provide through our website to third parties except as outlined in this policy and as otherwise permitted by law. We may share personal information with other third-party companies that we collaborate with or hire to perform services on our behalf. For example, we may hire a company to help us send and manage email, and we might provide the company with your email address and certain other information in order for them to send you an email message on our behalf. Similarly, we may hire companies to host or operate some of our websites and related computers and software applications. We may also share your personal information with third parties to permit them to send you marketing communications, if you have opted in to such sharing.

Additionally, we may share your information in other limited circumstances, including in response to a valid subpoena, warrant, or court order or as otherwise required by law or regulation or to cooperate with law enforcement authorities in investigating and prosecuting activities that are illegal, violate our rules, or may be harmful to other visitors. We may also share your information in the event of the sale or transfer of WPS or some of our assets, or in the context of similar transactions.

Security

While no system can provide guaranteed security, we take reasonable efforts to keep information you provide to us secure. We implement reasonable safeguards, including encryption technology and physical security at the location of the server where information is stored.



Guidance on Choosing a Third-Party Application and Your Right to Privacy

If you decide to access your information through the Patient Access API, you should carefully review the privacy policy of the third-party application you are considering using to ensure you are comfortable with what the app will do with your information. Remember the third-party application's use of your information will be governed by the third-party application privacy policies and terms and conditions.

Please note: WPS does not endorse or recommend the use or selection of any specific third-party application and you use the application at your own risk.

WPS is required to provide you with access to detailed information about your health data through a "Patient Access API." You may access this information by downloading a third-party application on your smartphone, tablet, computer, or other similar device. The information available through the Patient Access API includes information that WPS stores about you while you have been enrolled in your health plan. The data includes the following information while WPS maintained it in our records:

- Claims, clinical, and pharmacy data concerning your interactions with health care providers

The information WPS discloses may include information about treatment for substance use disorders, mental health treatment, HIV status, or other sensitive information.

Considerations in Choosing a Third-Party Application

The app you choose will have access to all of your personal information and is not subject to the Health Insurance Portability and Accountability Act (HIPAA), which generally protects the privacy and security of your health information. The app's privacy policy describes self-imposed limitations on how the app may use, disclose, and (possibly) sell information about you. It is important for you to know that once WPS sends your data to the app, WPS cannot control how the app secures, uses, or shares your information.

Things you may wish to consider when selecting a third-party application:

- Will the app sell my data for any reason and to whom?
- Will the app disclose my data to other third parties for purposes like research or advertising?
- For what purposes will this app use my data?
- Will the app allow me to control how it uses, releases, or markets my information?
- If I no longer want to use the app, or if I no longer want this app to have access to my health information, can I terminate the app's access to my data? If so, what is the process to terminate access?
- What is the app's policy for deleting my data once I terminate access? Do I have to do more than just delete the app from my device?
- How does the app inform consumers of changes in its privacy practices?

- Will the app collect non-health data from my device, such as my location, buying habits, etc.?
- What security practices does the app use to protect my data?
- What impact could sharing my data with the app have on others, such as my family members?
- Will the app permit me to access my data and correct inaccuracies? (Note that correcting inaccuracies in the app will not affect inaccuracies in the source of the data.)
- Does the app have a process in place for collecting and responding to user complaints?

It is important that you carefully review the app's privacy policy to ensure it addresses these types of questions, and that it has strong privacy and security standards to protect your information. If not, you may want to reconsider using that app to access your health information.

Consumer Privacy Protection Information

While not subject to HIPAA, apps are subject to certain federal and state consumer protection laws. If you believe an app used your information inappropriately or did not comply with its privacy and security policies, you may reach out to the U.S. Federal Trade Commission (FTC) or your state's consumer protection agency.

- [Locate your state's consumer protection agency.](#)
- [File a complaint with the FTC.](#)

Other Resources:

- [Federal Trade Commission \(FTC\)](#)
- [USA.gov identity theft website](#)
- [Consumer.gov identity theft website](#)

Covered Entities and HIPAA Enforcement

The U.S. Department of Health and Human Services' Office for Civil Rights (OCR) enforces the HIPAA Privacy, Security, and Breach Notification Rules. WPS Health Insurance and WPS Health Plan are subject to HIPAA, as are most health care providers, such as hospitals, doctors, clinics, and dentists. WPS has a Notice of Privacy Practices which explains how WPS uses and discloses your health information, as well as provides information on how you can request a copy of your health information directly from us or file a privacy complaint.

- [Nondiscrimination and Language Access Policy](#)
-

Website Analytics

When you browse through any website, certain information about your visit may be collected. WPS uses a web analytics program to collect information automatically and continuously. WPS uses this information to measure the number of visitors to its sites and to distinguish between new and returning visitors to help make the site more useful. However, no PII is collected.

WPS performs analyses of user behavior in order to measure customer interest in the various areas of our site. The reports are only available to limited staff that require this information in order to perform their job.

WPS website may also use online surveys to collect opinions and feedback from a random sample of visitors. This survey does not collect PII. Participation in the survey is voluntary. If you decline to participate, you will still have access to the identical information and resources on WPS' websites as those who do decide to take the survey. Answers to the survey help us to improve our provider websites to make them easier for you to use. WPS may utilize third-party vendors, such as Google Analytics and Foresee, to perform our web measurements and customizations.

How to WPS Uses Cookies

When you visit a website, its server may generate a piece of text known as a "cookie" to place on your computer. The cookie allows the server to "remember" specific information about your visit while you are connected. The cookie makes it easier for you to use the dynamic features of web pages. Requests to send cookies from WPS' web pages are designed to collect information about your browser session only; they do not collect personal information about you. Note that regardless of the particular uses for cookies on our website, we will not share any cookie information with any third parties.

There are two types of cookies: "Temporary session cookies" (single session) and "persistent cookies" (multi-session). Temporary session cookies will last only as long as your browser is open. Once you close your browser, the temporary session cookie will disappear. Persistent cookies are stored on your computer for longer periods.

How WPS Uses Persistent Cookies

WPS uses persistent cookies to help recognize new and returning visitors to WPS' websites. Persistent cookies remain on your computer between visits to the application websites until they expire. WPS does not use this technology to identify you or any other individual site visitor.

WPS websites may use persistent cookies to track language preferences. WPS also uses persistent cookies to enable its web analytics program to measure how new and returning visitors use WPS websites over time.

How to "Opt Out" or Disable Cookies

If you do not wish to have temporary or persistent cookies placed on your computer, you may disable them using your browser. If you decide to "opt out" of cookies, you will still have access to information and resources WPS websites provide, but you may be unable to fully use certain portions of the website.

You can remove any cookies that have been created in the cookie folder of the most popular internet browsers. Simply click the "Help" function on your browser and enter "cookies" to search for information on how to remove all or individual cookies.

Online Privacy Notice for Children

Our services are not directed to or intended for children. WPS does not knowingly collect or post information from children under the age of 13 in compliance with laws protecting the privacy of children.

Employment Applicants

We collect information, including personal contact information, education and work history, as well as Social Security and similar national identification numbers in order to process and consider your applications. We will not sell your application to unaffiliated third parties for marketing purposes. The information you provide WPS on your application may be shared with background check services and our affiliates and used for certain regulatory, compliance and legal purposes.

Social Media

WPS may maintain certain profiles and/or pages on various social media platforms, including Facebook, Twitter, and LinkedIn. If you choose to "Like," "Follow," or take any other similar action on a social media site, you are providing your consent to receive information updates, including solicitations, from WPS. To stop receiving this information from WPS on a social media site, you must follow the procedures established by the site to "Unlike" or "Unfollow" WPS' profile or page.

Links to Non-WPS Websites

WPS' websites may contain links to other websites. WPS is not responsible for the privacy practices or the content of those other websites.

Privacy Policy Updates

WPS reserves the right to modify this privacy policy at any time. We encourage visitors to frequently check this page for any changes to its Privacy Policy. Your continued use of this site after any change in this Privacy Policy will constitute your acceptance of such change.

Contacting the WPS Privacy Officer

WPS has a designated Privacy Officer who is available to answer privacy questions or for reporting privacy issues. You may contact the WPS Privacy Officer by submitting your comments or questions via email to: [Privacy Officer](#) or by mail to:

WPS—A health solutions company
Attention: WPS Privacy Officer
1717 W. Broadway
P.O. Box 8190
Madison, WI 53708-8190

- [View our Notice of Privacy Practices](#)
- [Aviso de prácticas de privacidad](#)

