Privacy Policy

Effective date: September 4, 2025

This privacy policy ("Privacy Policy") is entered into by and between you ("You" or "User") and Phanova, Inc., a Delaware corporation ("Company"). This Privacy Policy governs your access to and use of the Company's:

1. **Online and Mobile Services**
2. **Offline Services**
3. **Certain Tools:** This includes, but is not limited to, the generation of medical necessity letters, coverage guidance analysis, and medical knowledge summarizer.
4. **Company Software Applications:** This includes, but is not limited to, the Company's website (Phanova.com) and platform, as well as mobile applications provided by the Company (collectively referred to as the "Company Apps").

The term "Company Apps" encompasses, including, but not limited to, all content, functionality, and practice management services offered on or through the Company Apps.

This page informs you of our policies regarding the collection, use, and disclosure of personal data when you use our Company Apps and the choices you have associated with that data. This Privacy Policy is a legally binding agreement between you ("User", "you" or "your") and the Company. By accessing and using the Website and Company Apps, you acknowledge that you have read, understood, and agree to be bound by the terms of this Agreement. This Policy does not apply to the practices of companies that we do not own or control. This policy applies to all of our Company Apps.

We use your data to provide and improve the Company Apps. By using the Company Apps, you agree to the collection and use of information in accordance with this policy now and as amended by us. Unless otherwise defined in this Privacy Policy, terms used in this Privacy Policy have the same meanings as in our Terms of Use.

Definitions

- **Company Apps**: Company Apps means our online and/or mobile services and Company software applications, including but not limited to, the Company's Phanova.com website and Company Apps, and mobile applications provided by the Company and operated by us.
- **Personal Data**: Personal Data means data about a living individual who can be identified from that data (or from other information either in our possession or likely to come into our possession).
- **Usage Data**: Usage Data is data collected automatically either generated by the use of the Company Apps or from the Company Apps infrastructure itself (for example, the duration of a page visit).
- **Cookies**: Cookies are small pieces of data stored on your device (computer or mobile device).
- **Data Controller**: Data Controller means the natural or legal person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal information are, or are to be, processed. For the purpose of this Privacy Policy, we are a Data Controller of your Personal Data.

- **Data Processors (or Service Providers)**: Data Processor (or Service Provider) means any natural or legal person who processes the data on behalf of the Data Controller. We may use the services of various Service Providers in order to process your data more effectively.
- **Data Subject (or User)**: Data Subject is any living individual who is using our Company Apps and is the subject of Personal Data.

General Information Collection and Use

We collect several different types of information for various purposes to provide and improve our Company Apps to you. Our information collection includes using cookies on a computer/handheld device or using or touching information in any way, including, but not limited to, collecting, storing, deleting, using, combining and disclosing information, all of which activities will take place in the United States. If you reside outside the United States your information will be transferred, processed and stored there under United States privacy standards.

Specific Information Collection and Use

Through our Company Apps, we may collect and utilize information from users:

- User ID.
- Encrypted patient identifier.
- Hash signature of clinical information.
- Requested medical service (e.g., drug, procedure or device).
- Which carrier are they asking to cover the service?
- Medical information about the patient (whether the user or someone else else) which will be anonymized before persistence in the Company Apps' database.
- Run the Company Apps: Conclusions and determinations (e.g., medical necessity and coverage criteria satisfaction) derived from an anonymized version of the clinical information.
- Train and test artificial intelligence models: Specifically, train generative models of patient information (i.e., learning how to fabricate a patient record) from the anonymized patient record and information extraction/reasoning models (i.e. determining whether a given medical information satisfies a given clinical criterion).
- Derive insights about user behaviors and requests (which services, which insurers etc.)

Artificial Intelligence (AI) Information Collection and Use

We may use AI on our Company Apps to enhance your user experience and provide various services.

The fundamental functionality and value proposition of our products hinge on advanced AI technology. Specifically designed to optimize and elevate the user experience, our AI models play an integral role in enhancing the quality and efficiency of our Company Apps. Understanding medical information, health insurance requirements and their interaction, and optimizing overall functionality are intrinsic tasks that form the core capabilities of our products, without which certain tasks may become impractical or significantly less efficient.

Please note that the use of AI may result in the collection and analysis of data related to your activities on our Company Apps. This data may include information such as your location, device information, IP address, and other relevant details.

Rest assured that we are committed to safeguarding your privacy and ensuring the security of your data.

Types of Data Collected

Personal Data

While using our Company Apps, we may ask you to provide us with certain personally identifiable information that can be used to contact or identify you ("Personal Data"). Personally identifiable information may include, but is not limited to:

- Account Registration Information
- Email address
- First name and last name
- Cookies and Usage Data
- IP addresses of individuals when using the Company Apps
- Phone Numbers - SMS

Usage Data

We may also collect information that your browser sends whenever you visit our Company Apps or when you access the Company Apps by or through a mobile device. This Usage Data may include information such as your computer's Internet Protocol address (e.g. IP address), browser type, browser version, the pages of our Company Apps that you visit, the time and date of your visit, the time spent on those pages, unique device identifiers and other diagnostic data. When you access the Company Apps by or through a mobile device, this Usage Data may include information such as the type of mobile device you use, your mobile device unique ID, the IP address of your mobile device, your mobile operating system, the type of mobile Internet browser you use, unique device identifiers and other diagnostic data.

Location Data

We may use and store information about your location if you give us permission to do so ("Location Data"). We use this data to provide features of our Company Apps, to improve and customize our Company Apps. You can enable or disable location services when you use our Company Apps at any time, through your device settings.

Tracking & Cookies Data

We use cookies and similar tracking technologies to track the activity on our Company Apps and hold certain information. Cookies are files with small amount of data which may include an anonymous unique identifier. Cookies are sent to your browser from a website and stored on your device. Tracking technologies also used are beacons, tags, and scripts to collect and track information and to improve and analyze our Company Apps. You can instruct your browser to refuse all cookies or to indicate when a cookie is being sent. However, if you do not accept cookies, you may not be able to use some portions of our Company Apps.

Examples of Cookies we use:

- **Session Cookies.** We use Session Cookies to operate our Company Apps.
- **Preference Cookies.** We use Preference Cookies to remember your preferences and various settings.
- **Security Cookies.** We use Security Cookies for security purposes.

Use of Data

Company may use the collected data for various purposes, including, but not limited to:

- To provide and maintain our Company Apps
- To notify you about changes to our Company Apps
- To allow you to participate in interactive features of our Company Apps when you choose to do so
- To provide customer support
- To gather analysis or valuable information so that we can improve our Company Apps
- To monitor the usage of our Company Apps
- To detect, prevent and address technical issues

Retention of Data

Company will use commercially acceptable means to retain your Personal Data only for as long as is necessary for the purposes set out in this Privacy Policy. We will use commercially acceptable means to retain and use your Personal Data to the extent necessary to comply with our legal obligations (for example, if we are required to retain your data to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies. Company will also retain Usage Data for internal analysis purposes. Usage Data is generally retained for a shorter period of time, except when this data is used to strengthen the security or to improve the functionality of our Company Apps, or we are legally obligated to retain this data for longer time periods.

Transfer of Data

Your information, including Personal Data, may be transferred to — and maintained on — computers located outside of your state, province, country or other governmental jurisdiction where the data protection laws may differ than those from your jurisdiction. If you are located outside United States and choose to provide information to us, please note that we may transfer the data, including Personal Data, to United States and process it there. Your consent to this Privacy Policy followed by your submission of such information represents your agreement to that transfer. Company will use commercially acceptable means to ensure that your data is treated securely and in accordance with this Privacy Policy and no transfer of your Personal Data will take place to an organization or a country unless there are adequate controls in place including the security of your data and other personal information.

Business Transaction

If Company is involved in a merger, acquisition or asset sale, your Personal Data may be transferred. We will use commercially acceptable means to provide notice before your Personal Data is transferred and becomes subject to a different Privacy Policy.

Disclosure for Law Enforcement

Under certain circumstances, Company may be required to disclose your Personal Data if required to do so by law or in response to valid requests by public authorities (e.g. a court or a government agency).

Legal Requirements

Company may disclose your Personal Data in the good faith belief that such action is necessary to:

- To comply with a legal obligation
- To protect and defend the rights or property of Phanova, Inc.
- To prevent or investigate possible wrongdoing in connection with the Company Apps
- To protect the personal safety of users of the Company Apps or the public
- To protect against legal liability

Security of Data

Broadly, security measures include:

1. Using a HIPAA-compliant managed database for storing patient data.
2. Using identity providers for authentication.
3. Refraining from saving identifiable patient information in the database.
4. De-identifying patient information before it leaves the user's computer.
5. Using a managed service for running the front-end (user-facing) and backend application servers.
6. Using a HIPAA-compliant vendors for artificial intelligence model execution.

The security of your data is important to us but remember that no method of transmission over the Internet, or method of electronic storage is 100% secure. While we strive to use commercially acceptable means to protect your Personal Data, we cannot guarantee its absolute security.

California Online Privacy Protection Act (CalOPPA)

We do not support Do Not Track ("DNT"). Do Not Track is a preference you can set in your web browser to inform websites that you do not want to be tracked. You can enable or disable Do Not Track by visiting the Preferences or Settings page of your web browser. In addition to the rights as explained in this Policy, California residents who provide Personal Information (as defined in the statute) to obtain products or services for personal, family, or household use are entitled to request and obtain from us, once a calendar year, information about the Personal Information we shared, if any, with other businesses for marketing uses. If applicable, this information would include the categories of Personal Information and the names and addresses of those businesses with which we shared such personal information for the immediately prior calendar year (e.g., requests made in the current year will receive information about the prior year). To obtain this information please contact us.

Your Data Protection Rights Under General Data Protection Regulation (GDPR)

If you are a resident of the European Economic Area (EEA), you have certain data protection rights. Company aims to take commercially acceptable steps to allow you to correct, amend, delete, or limit the use of your Personal Data. If you wish to be informed what Personal Data we hold about you and if you want it to be removed from our systems, please contact us.

In certain circumstances, you have the following data protection rights:

- **The right to access, update or to delete the information we have on you.** Whenever made possible, you can access, update or request deletion of your Personal Data directly within your account settings section. If you are unable to perform these actions yourself, please contact us to assist you.
- **The right of rectification.** You have the right to have your information rectified if that information is inaccurate or incomplete.
- **The right to object.** You have the right to object to our processing of your Personal Data.
- **The right of restriction.** You have the right to request that we restrict the processing of your personal information.
- **The right to data portability.** You have the right to be provided with a copy of the information we have on you in a structured, machine-readable and commonly used format.
- **The right to withdraw consent.** You also have the right to withdraw your consent at any time where Company relied on your consent to process your personal information.

Please note that we may ask you to verify your identity before responding to such requests. You have the right to complain to a Data Protection Authority about our collection and use of your Personal Data. For more information, please contact your local data protection authority in the European Economic Area (EEA).

Service Providers

We may employ third party companies and individuals to facilitate our Company Apps ("Service Providers"), to provide the Company Apps on our behalf, to perform Company Apps-related services or to assist us in analyzing how our Company Apps is used. These third parties have access to your Personal Data only to perform these tasks on our behalf and are obligated not to disclose or use it for any other purpose. Here are some of the Service Providers we use:

- **Microsoft Authenticator**: The Microsoft Authenticator app helps you sign in to your accounts when you're using two-step verification.

  You can learn more about Microsoft Authenticator by visiting this page: https://privacy.microsoft.com/en-us/privacystatement

- **Auth0:** Auth0 is a secure identity cloud that links all your apps, logins and devices into a unified digital fabric.

  You can learn more about the privacy practices and policies of Okta by visiting their Privacy Policy page: www.okta.com/privacy-policy/

- **OpenAI:** We use OpenAI for artificial intelligence models: for analyzing the data.

  You can learn more about the privacy practices and policies of OpenAI by visiting their Privacy Policy page: https://openai.com/enterprise-privacy

- **Anthropic:** We use Anthropic for artificial intelligence models: for analyzing the data.

  You can learn more about the privacy practices and policies of Anthropic by visiting their Privacy Policy page: https://privacy.claude.com/en/

- **Microsoft Azure:** We use Microsoft Azure for application hosting, artificial intelligence models (for analyzing the data) and database services that is running the product and storaing data.

  You can learn more about the privacy practices and policies of Microsoft Azure by visiting their Privacy Policy page: https://privacy.microsoft.com/en-us/privacystatement
- **Microsoft Azure:** We use Amazon Web Services for application hosting, artificial intelligence models (for analyzing the data) and database services that is running the product and storing data.

  You can learn more about the privacy practices and policies of Amazon Web Services by visiting their Privacy Policy page: https://aws.amazon.com/privacy/

Payments

We may provide paid products and/or services within the Company Apps. In that case, we use third-party services for payment processing (e.g. payment processors). We will not store or collect your payment card details. That information is provided directly to our third-party payment processors whose use of your personal information is governed by their Privacy Policy. These payment processors adhere to the standards set by PCI-DSS as managed by the PCI Security Standards Council, which is a joint effort of brands like Visa, Mastercard, American Express and Discover. PCI-DSS requirements help ensure the secure handling of payment information.

Links to Other Sites

1. Our Company Apps may contain links to other sites that are not operated by us, which include Medical knowledge bases such as pubmed.gov. and health insurers' websites/materials such as Medicaid, Medicare, Aetna etc. If you click on a third-party link, you will be directed to that third party's site. We strongly advise you to review the Privacy Policy of every site you visit. We have no control over and assume no responsibility for the content, privacy policies or practices of any third-party sites or services.

Children's Privacy

Our Company Apps does not address anyone under the age of 18.

We do not knowingly collect personally identifiable information from anyone under the age of 18. If you are a parent or guardian and you are aware that your child has provided us with Personal Data, please contact us. If we become aware that we have collected Personal Data from children without verification of parental consent, we will take steps to remove that information from our servers.

Changes to This Privacy Policy

We may update our Privacy Policy from time to time. We will notify you of any changes by posting the new Privacy Policy on this page. You are advised to review this Privacy Policy periodically for any changes. Changes to this Privacy Policy are effective when they are posted on this page.

Contact Us

If you have any questions about this Privacy Policy, please contact us:

- By email: privacy@Phanova.com