Effective Date: January 9, 2024

Bloom for Women LLC, d/b/a Noble Health App Privacy Policy

PRIVACY POLICY

This Privacy Policy ("Policy") governs the use of client Personal Data. Please read this Policy carefully regarding the Company's practices and procedures as to such Personal Data.

INTRODUCTION

Bloom for Women LLC, d/b/a Noble Health App (hereinafter, "Noble") (referred to as "the Company", "We", "Us") values client privacy. The Company is likewise committed to keeping client personal data confidential. Such data is used solely for purposes of providing clients services through access to the Noble web portal and the Noble app (collectively referred to as the "Platform"). The data allows Noble to provide content and functionality (the "Services") to qualified medical providers ("Provider Users") and patients ("Patient Users"). All persons utilizing the Services are classified as either Provider Users or Patient Users. Users are sometimes referred to by "You" or Your" in this Policy.

This Policy applies to Personal Data that the Company collects from users of the Platform and the Services. **"Personal Data" consists of all information which, independently or in connection with other information, could be used to identify a user.** This Policy seeks to provide transparency about how Personal Data is used. For that reason, this Policy gives users detailed explanations about the Company's collection, use, maintenance, and disclosure of Personal Data. This includes how Personal Data is collected, used and protected, and user's rights regarding Personal Data.

SUMMARY

PURPOSES FOR COLLECTING PERSONAL DATA

PURPOSE	HOW COLLECTED
Provision of Services under the Terms of Service	Users agree upon registration (checkbox)
Patient communications, User account management	Email, text messaging, phone call, Zendesk, platform messaging
Data storage	RDS database
Responding to information requests from governmental authorities, or for legal proceedings	Zendesk
Technical support for users	Zendesk
Operations management for the Platform	AWS IAM
User payment processing	Stripe
Security of the Platform	AWS IAM

TYPES OF PERSONAL DATA COLLECTED

TYPE OF DATA	HOW COLLECTED
Demographic Data (birth year, gender, height, weight, phone number, and email address)	Django database, Typeform
Payment Data (billing name and address, credit card number or bank account information)	Stripe
Data needed to provide support (e.g., Internet IP address)	Contact info. Generally name, email address and phone number.
Device and ISP Data (IP address (or proxy server), device and application identification numbers, location, browser type, Internet service provider and/or mobile carrier, the pages and files You viewed, Your searches, Your operating system and system configuration information, and date/time stamps associated with Your usage)	N/A
Health and Device Data of Patient Users (health conditions, including medical history, symptoms, physiologic data recorded by our Devices, and communications between You and the healthcare provider providing healthcare services to You via the Platform)	Django database

THIRD PARTIES DATA IS SHARED WITH

TYPE OF DATA	THIRD PARTIES RECEIVING
Personal data of Patient Users	Healthcare providers will have access to their patient's progress in the program via the Noble platform

MORE DETAILS ABOUT THESE POLICIES ARE SET FORTH IN SECTIONS 3-8 BELOW.

YOUR OPT-OUT AND OTHER RIGHTS CONCERNING DATA COLLECTION AND USE ARE SET FORTH IN SECTION 9 BELOW.

POLICY

1. SPECIFIC ITEMS FOR PATIENT USERS

a. Some Personal Data collected may be "HEALTH DATA" (data regarding Your physical or mental health), "PROTECTED HEALTH INFORMATION" or "PHI" (data regarding Your past, present, or future physical or mental health or condition(s); Your medical treatment; Your past, present, or future payment for medical treatment), and/or MEDICAL RECORDS as defined by federal and/or state law. For this reason, this Policy is intended to comply with the federal Health Insurance Portability And Accountability Act of 1996 ("HIPAA") and affected state law(s) regarding the use and disclosure of PHI and related subject matter. If there are additional concerns about this, please contact the Company's privacy officer, Eric Red, at privacy@noble.health.

b. Because Noble cares about the safety and privacy of children online, we comply with the Children's Online Privacy Protection Act of 1998 (COPPA). COPPA and its accompanying FTC regulation establish United States federal law that protects the privacy of children using the Internet. We do not knowingly contact or collect personal information from children under 13. Our site is not intended to solicit information of any kind from children under 13. It is possible that by fraud or deception we may receive information pertaining to children under 13. If we are notified of this, as soon as we verify the information, we will immediately obtain parental consent or otherwise delete the information from our servers. If you want to notify us of our receipt of information by children under 13, please contact us.

To further protect Users between the ages of 13 and 18, a parent or legal guardian must affirm agreement to use of the Services by the underage Patient. A specific step in the registration process as referred to in the accompanying Terms of Use will collect this information, and Noble will rely upon the information collected as being truthful and accurate.

c. ***BY SUBMITTING YOUR PERSONAL DATA THROUGH THE PLATFORM, YOU ARE ACKNOWLEDGING THAT YOU HAVE READ AND AGREE TO THE TERMS OF THIS POLICY. IF YOU DO NOT AGREE, PLEASE DO NOT SUBMIT ANY PERSONAL DATA TO US AND IMMEDIATELY CEASE USE OF THE SERVICES.***

d. This Policy is updated periodically and the version displayed on the Portal will always be the most current version. We will post a notice on the Portal that the Policy has been updated, and/or email You a link to the updated version using an email address You have provided to Us. It is Your responsibility to familiarize yourself with amendments. Changes to this Policy will be effective immediately upon providing notice, and apply to all personal data We maintain, use, and disclose. If you continue to use the Services following such notice, You are agreeing to those changes.

e. If at any point You no longer agree to the use and disclosure of Personal Data, as described in this Policy, You can delete Your account by requesting deletion. To do so, email hello@noble.health with the subject line "REQUEST FOR PERSONAL DATA DELETION" and request that Your account be deleted.

2. WHO IS RESPONSIBLE FOR YOUR DATA?

The Company controls Your Personal Data and may process the data consistent with this Policy. In any instance in which the Company processes Personal Data on behalf of a third party that is not an agent or affiliate of Company, that is controlled by the third party's privacy policy, and this Policy will not apply. Questions about this should be directed to hello@noble.health.

The Platform may contain links to websites or services owned or operated by third parties (each, a "Third-Party Service"). Any information that You provide in connection with a Third-Party Service is provided directly to the owner or operator of the Third-Party Service, subject to the owner's or operator's privacy policy. The Company is not responsible for the content, privacy or security practices and policies of any Third-Party Service. To protect Your information, We recommend that You carefully review the privacy policies of all Third-party Services that You access.

3. WHAT PERSONAL DATA DO WE COLLECT?

a. Demographic Data. We may collect demographic information, such as Your name, birth year, gender, height, weight, phone number, and email address, and if you are a Provider User, Your National Provider Identifier ("NPI"). Primarily, the collection of Your Personal Data assists Us in creating Your User Account, which You can use to securely receive the Services.

b. Payment Data. If You make payments via the Platform, We may require that You provide Your financial and billing information, such as billing name and address, credit card number or bank account information.

c. Data Required for Support. If You contact Us for support or to submit a complaint, We may collect technical or other information from You through log files and other technologies, some of which may qualify as Personal Data. (for example, Your internet IP address). This information will be used for the purposes of troubleshooting, customer support, software updates, and improvement of the Platform and related Services in accordance with this Policy.

d. Device and ISP Data. We use information-gathering tools, such as log files, cookies, Web beacons, and similar technologies to automatically collect information, which may contain Personal Data, from Your computer or mobile device as You use the Platform or interact with emails We have sent You. The information We collect may include Your IP address (or proxy server), device and application identification numbers, location, browser type, Internet service provider and/or mobile carrier, the pages and files You viewed, Your searches, Your operating system and system configuration information, and date/time stamps associated with Your usage. This information is used to analyze overall trends, to help Us provide and improve Our Services and to guarantee their security and continued proper functioning.

e. Health and Device Data (for Patient Users). In addition to demographic information, We may collect information regarding Your health conditions, including medical history, symptoms, physiologic data recorded by our Devices, and communications between You and the healthcare provider providing healthcare services to You via the Platform. We collect this information to provide You with the Services and to provide Your healthcare provider providing healthcare services through the Platform with the information required to provide medical treatment.

4. HOW WILL WE USE YOUR PERSONAL DATA?

We use Your Personal Data based on legitimate business interests, the fulfillment of Our Services to You, compliance with Our legal obligations, and/or Your consent. We only use or disclose Your Personal Data when it is legally mandated or where it is necessary to fulfill those purposes described herein. Where required by law, We will ask for Your prior consent before doing so.

a. The legitimate business purposes for which the Personal Data is used are:

i. To fulfill Our obligations to You under Our Terms of Use: https://noble.health/consent/

ii. To communicate with You about and manage Your User Account

iii. To store and track Your data within Our system

iv. To respond to lawful requests from public/governmental authorities, and/or to comply with applicable state/federal law, including cooperation with judicial proceedings or court orders

v. To protect Your/Our/third-party's rights, privacy, safety, or property, by providing proper notices, pursuing available legal remedies, or acting to limit Our damages

vi. To handle technical support and other requests from You

vii. To ensure compliance with Our Terms of Use or the terms of any other applicable services agreement We have with You

viii. To manage and improve Our operations and the Platform, including the development of additional functionality

ix. To manage payment processing

x. To evaluate the quality of service You receive, identify usage trends, and thereby improve Your user experience

xi. To keep Our Platform safe and secure

xii. To send You information about changes to Our terms, conditions, and policies

xiii. To allow Us to pursue available remedies or limit the damages that We may sustain

xiv. If you are a Patient User, to enable You to connect with (or share Personal Data with) the authorized Provider User to enable that individual to monitor Your progress and overall condition, as such Provider User deems appropriate

b. Personal Data We collect through the Platform and Devices will be stored on secure servers. Personal Data may be transmitted to third parties, which parties may store or maintain the data on their secure servers.

c. Personal Data may be shared with third parties in certain instances:

i. Personal Data of Patient Users will be shared with Provider User(s) that You have connected with as part of the Services. You can deny access to Provider Users by emailing hello@noble.health.

ii. Personal Data of Patient Users may be shared with service providers and other third parties ("Business Partners") that help Us run various aspects of Our business. These Business Partners are contractually bound to protect Your Personal Data and to use it only for the limited purpose(s) for which it is shared with Us. Business Partners' use of Personal Data may include, but is not limited to, the provision of services such as data hosting, IT services, customer service, and payment processing.

iii. Personal Data of Patient Users may be shared to (A) comply with legal processes or enforceable governmental requests, or as otherwise required by law; (B) cooperate with third parties in investigating acts or omissions that violate this Policy or the Terms of Use; or (C) bring legal action against someone who may be violating the Terms of Use or who may be causing intentional or unintentional injury or interference to the rights or property of Noble, , including other users of Our Services.

iv. Personal Data of Patient Users may be shared with advisory services providers to the Company, such as lawyers, auditors, accountants, or banks, when We have a legitimate business interest in doing so.

v. Personal Data of Patient Users may be shared with third parties in the event of a reorganization, merger, sale, joint venture, assignment, transfer, or other disposition of all or any portion of Noble's assets or membership interest (including in connection with any bankruptcy or similar proceedings).

d. ***If We share Your Personal Data with a third party other than as provided above, You will be notified at the time of data collection or transfer, and You will have the option of not permitting the transfer.***

5. HOW LONG DO WE RETAIN PERSONAL DATA?

a. We will retain Your Personal Data for as long as You maintain a User Account and up to six years after the account is closed. The exact period of retention will depend on the type of Personal Data, Our contractual obligation to You, and applicable law. We keep Your Personal Data for as long as necessary to fulfill the purpose for which it was collected, unless otherwise required or necessary pursuant to a legitimate business purpose outlined in this Policy. At the end of the applicable retention period, We will remove Your Personal Data from Our databases and will request that Our Business Partners remove Your Personal Data from their databases. If there is any data that We are unable, for technical reasons, to delete entirely from Our systems, We will put in place appropriate measures to prevent any further processing of such data. We retain anonymized data indefinitely.

b. Once We disclose Your Personal Data to third parties, We may not be able to access that Personal Data any longer and cannot force the deletion or modification of any such information by the parties to whom We have made those disclosures. Written requests for deletion of Personal Data other than as described should be directed to hello@noble.health.

6. OUR POLICY REGARDING COOKIES

Cookies are small files that a web server sends to Your computer or device when You visit a web site that uses cookies to keep track of Your activity on that site. Cookies also exist

within applications when a browser is needed to view certain content or display certain content within the application. Cookies hold a small amount of data specific to that website, which can later be used to help remember information You enter into the site (like Your email or other contact info), preferences selected, and movement within the site. If You return to a previously visited web site or application (and Your browser has cookies enabled), the web browser sends the small file to the web server, which tells it what activity You engaged in the last time You used the web site or application, and the server can use the cookie to do things like expedite logging in and retrieving user data and keeping Your browser session secure.

a. We use cookies and other technologies to, among other things, better serve You with more tailored information, and to facilitate efficient and secure access to the Platform. We only use essential cookies, which are cookies necessary for Us to provide the Services. You may disable cookies on a browser as set forth below but doing so may affect the functionality of the Services.

b. We may also collect information using pixel tags, web beacons, clear GIFs, or other similar technologies. These may be used in connection with some web site or application pages and HTML-formatted email messages to, among other things, track the actions of users and email recipients, and compile statistics about usage and response rates.

c. If You prefer, You can usually choose to set Your browser to remove cookies and reject cookies. If You enable a do not track ("DNT") signal or otherwise configure Your browser to prevent Noble from collecting cookies, You will need to reenter Your user name each time You visit the login page.

7. HOW DO WE PROTECT YOUR PERSONAL DATA?

a. Noble is committed to protecting the security and confidentiality of Your Personal Data. We use a combination of reasonable physical, technical, and administrative security controls to maintain the security and integrity of Your Personal Data, to protect against any anticipated threats or hazards to the security or integrity of such information, and to protect against unauthorized access to or use of such information in Our possession or control that could result in substantial harm or inconvenience to You. However, Internet data transmissions, whether wired or wireless, cannot be guaranteed to be 100% secure. As a result, We cannot ensure the security of information You transmit to Us. By using the Platform, You are assuming this risk as to all Personal Data.

b. The information collected by Noble and stored on secure servers, is protected by a combination of technical, administrative, and physical security safeguards, such as authentication, encryption, backups, and access controls. If Noble learns of a security concern, We may attempt to notify You and provide information on protective steps, if available, through the email address that You have provided to Us. Depending on where You live, You may have a legal right to receive such notices in writing.

c. You are solely responsible for protecting information entered or generated via the Platform that is stored on Your device and/or removable device storage. Noble has no access to or control over Your device's security settings, and it is up to You to implement any device level security features and protections You feel are appropriate (for example, password protection, encryption, two factor authentication, remote wipe capability, etc.). We recommend that You take any and all appropriate steps to secure any device that You use to access Our Platform.

d. ***NOTWITHSTANDING ANY OF THE STEPS TAKEN BY US, IT IS NOT POSSIBLE TO GUARANTEE THE SECURITY OR INTEGRITY OF DATA TRANSMITTED OVER THE INTERNET. THERE IS NO GUARANTEE THAT YOUR PERSONAL DATA WILL NOT BE ACCESSED, DISCLOSED, ALTERED, OR DESTROYED DESPITE THE IMPLEMENTATION OF OUR PHYSICAL, TECHNICAL, OR ADMINISTRATIVE SAFEGUARDS. THEREFORE, WE DO NOT AND CANNOT ENSURE OR WARRANT THE SECURITY OR INTEGRITY OF ANY PERSONAL DATA YOU TRANSMIT TO US AND YOU TRANSMIT SUCH PERSONAL DATA AT YOUR OWN RISK.***

e. In instances where You have authorized the Company to use and disclose Your Personal Data for certain purposes, You may withdraw Your consent in the future. You may withdraw Your consent by sending a request in writing to: support@noble.heath or Noble Health, Attn: Website Support, 199 North 290 West, Ste. 150, Lindon, UT 84043. Your withdrawal will not be effective until We receive Your request and will not apply to uses and disclosures that We have already made in reliance on Your consent.

8. HOW CAN YOU PROTECT YOUR PERSONAL DATA?

a. In addition to securing Your device, as discussed above, be advised that Noble will NEVER send You an email requesting confidential information such as account numbers, usernames, passwords, or social security numbers, and You should NEVER respond to any email requesting such information. ***If You receive such an email that looks like it is from Noble, DO NOT RESPOND to the email and DO NOT click on any links and/or open any attachments in the email.*** Notify Noble support at hello@noble.health.

b. You are responsible for taking reasonable precautions to protect Your user ID, password, and other User Account information from disclosure to third parties, and You are not permitted to circumvent the use of required encryption technologies. You should immediately notify Us at hello@noble.health if You know of or suspect any unauthorized use or disclosure of Your user ID, password, and/or other User Account information, or any other security concern.

9. YOUR RIGHTS

You have certain rights relating to Your Personal Data, subject to applicable data protection laws. These rights may include:

i. to access Your Personal Data held by Us

ii. to erasure/deletion of Your Personal Data, to the extent permitted by applicable data protection laws

iii. to receive communications related to the processing of Your Personal Data that are concise, transparent, intelligible, and easily accessible

iv. to restrict the processing of Your Personal Data, to the extent permitted by law (while We verify or investigate Your concerns with this information)

v. to object to the further processing of Your Personal Data, including the right to object to marketing

vi. to request that Your Personal Data be transferred to a third party, if possible

vii. to receive Your Personal Data in a structured, commonly used, and machine-readable format

viii. to lodge a complaint with a supervisory authority

ix. to rectify inaccurate Personal Data and, taking into account the purpose of processing the Personal Data, ensure it is complete

x. to not be subject to a decision based solely on automated processing, including profiling, which produces legal effects ("Automated Decision-Making")

a. Where the processing of Your Personal Data by Us is based on consent, You have the right to withdraw that consent without detriment at any time or to exercise any of the rights listed above by emailing Us at hello@noble.health.

b. Updating, correcting, or deleting Personal Data

i. You can change Your email address and other contact information by contacting us at hello@noble.health. If You need to make changes or corrections to other information, You may contact us at hello@noble.health. Please note that in order to comply with certain requests to limit use of Your Personal Data, We may need to terminate Your account and Your ability to access and use the Services, and You agree that We will not be liable to You for such termination, or for any refunds of prepaid fees paid by You. You can deactivate Your account by request at hello@noble.health.

ii. Although We will use reasonable efforts to do so, You understand that it may not be technologically possible to remove from Our systems every record of Your Personal Data. The need to back up Our systems to protect information from inadvertent loss means a copy of Your Personal Data may exist in a non erasable form that will be difficult or impossible for Us to locate or remove.

c. Opt out of communications from Noble

We will not market third party services to You without Your consent. We only send emails to You regarding Your account unless We have Your express consent to do otherwise. You can choose to filter these emails using Your email client settings, but We do not provide an option for You to opt out of these emails.

d. Information submission by minors

We do not knowingly collect Personal Data from individuals under the age of 18. Our Services are not directed to individuals under the age of 18, except with express permission of the individual's parent or legal guardian. We request that these individuals not provide Personal Data to Us, unless the parent or legal guardian has consented to the same and provided the required affirmation of age and permissions set forth in the Noble Terms of Use. If We learn that Personal Data from users less than 18 years of age has been collected, and that the other aforementioned conditions are not met, We will deactivate the account and take reasonable measures to promptly delete such data from Our records.

If You are aware of a user under the age of 18 using the Web Site, please contact Us at hello@noble.health. Noble will internally confirm that the aforementioned conditions have been met, or will take other appropriate action(s) consistent with this Privacy Policy and the Terms of Use.

If You are a resident of California under the age of 18 and have registered for an account with Us, You may ask Us to remove content or information that You have posted to Our Platform.

e. California Residents

California residents may request and obtain from Us, once a year, free of charge, a list of third parties, if any, to which We disclosed their Personal Data for direct marketing purposes during the preceding calendar year and the categories of Personal Data shared with those third parties. If You are a California resident and wish to obtain that information, please submit Your request by sending Us an email at hello@noble.health with "California Privacy Rights" in the subject line.

10. CONTACT US WITH ADDITIONAL QUESTIONS OR CONCERNS

If You have any questions about this Policy, please contact Us by email at hello@noble.health, or write to Us at Noble Health, 199 North 290 West, Ste. 150, Lindon, UT 84043. ***Please note that email communications are not always secure; so please do not include sensitive information in Your emails to Us.***