Publish Date: November 11, 2025
Effective Date: November 13, 2025

b.well

Privacy Policy

Table of Contents

We encourage you to read this Privacy Policy from top to bottom, or to use the internal links provided to read specific sections. We've also included easy-to-read takeaway summaries within each section. Please take care not to rely on the section headings or takeaways: they are intended for reference and convenience only. They are not considered in how this Privacy Policy is to be interpreted.

---

1. Introduction

What is this Privacy Policy for?

This Privacy Policy describes the privacy commitments and data practices for the applications and digital experiences that b.well Connected Health, Inc. makes available under the b.well brand. We encourage you to read this Privacy Policy from top-to-bottom. But for a general overview, easy-to-read takeaways like this paragraph are included under each Heading.

The applications and digital experiences that b.well Connected Health, Inc. (alternately, "b.well", "we", "us" or "our") makes available under the b.well brand collect personal and sensitive data. This Privacy Policy ("Privacy Policy") provides detailed information about our privacy and data practice commitments concerning this data. Specifically, this Privacy Policy explains how we collect, create, use, process and share personally identifiable information in any website, mobile application, or interactive feature that links to this Privacy Policy and the b.well Terms of Service ("Terms"), specifically our b.well-branded https://portal.icanbwell.com/#/ website and mobile application (collectively, the "b.well application").

If you are using an online or mobile application that is offered by a b.well enterprise customer, and is governed by that customer's terms and privacy policy, then this Privacy Policy and the Terms do not apply. Instead, the Privacy and Security Statement for b.well enterprise customers and their end users applies.

The Terms include defined terms that we use in this Privacy Policy. While the Privacy Policy is a separate document, it should be read as part of the Terms. Conflicts or inconsistencies between this Privacy Policy and the Terms will be interpreted with precedence given to the Privacy Policy with respect to its subject matter.

This Privacy Policy also incorporates the b.well Tracking Technology Policy (the "Tracking Technology Policy"), which discusses b.well's use of tracking technologies in the b.well application to collect data from your devices when you interact with b.well digital properties. The Tracking Technology Policy is a supplement to this Privacy Policy and should be interpreted with precedence given to the Tracking Technology with respect to its subject matter. Specifically, the Tracking Technology Policy describes the tracking technologies that b.well uses to manage our interactions with you, and our commitment not to use vendors that use or sell your data in conflict with this Privacy Policy. It also provides information to help you understand how unrelated third parties may use tracking technologies to monitor your usage of b.well digital properties, and different steps you can take to limit these third parties from collecting this information.

We may provide additional privacy notices and affirmative, opt-in consents that supplement or amend the information contained in this Privacy Policy. Some of these notices are listed under Additional Privacy Notices. You can access other notices and your consent settings in your account in the b.well application (your "b.well account").

We encourage you to read this Privacy Policy from top to bottom, or to use internal links to read specific sections. We've also included easy-to-read takeaways under each section.

2. Categories of Data We Collect

What types of data are covered by this Privacy Policy?
We use defined terms to explain the data covered by this Privacy Policy. These categories of data include personal and sensitive data. This Privacy Policy includes disclosures about how and why b.well accesses, collects, uses and shares your personal and sensitive data, and when you have choices about these practices.

We collect the Personal Data described more fully below. "**Personal Data"** means any information that can be used to identify you or a member of your family or household.

Personal Data includes any data from whatever source and in whatever form or medium that is linked to your b.well account. Personal Data can include information from different sources that relates to health status, non-medical factors that could influence health, the healthcare services or resources that are either available or used by you, or the payment or cost for healthcare by you or others in your family (collectively, "**Health Data"**).

Below is a list of different types of Personal Data, including Health Data, that is covered by this Privacy Policy:
Data You Enter Directly. Any information you share with the b.well application through your b.well account. This can include demographic information, and other self-reported data that you enter manually; for example, by completing forms, surveys, or conducting other activities within the application.

Passive Data. Any information that the b.well application collects passively from your device or browser or your interactions with the application. This information includes, but is not limited to, data about the browser or device you use to access and use the b.well application, such as your IP Address. Passive Data can also be tiny graphics, data, or code that we embed in the software that delivers the application. For more information, read the Tracking Technologies Policy.

Device Data. Any information that we access through permissions with your device's operating system, such as your location data, or images captured by your device's camera. Typically, we will collect your consent before accessing a particular type of device data. For more information, read the Tracking Technologies Policy.

ePHR Data. Any copy of Health Data that is available for you to access under your direction through a Health Data Connection (defined below). Typically, ePHR Data is a subset of information from medical records that third party healthcare organizations maintain because of your current or past relationship as a patient or plan member. For example, you may be able to collect ePHR Data from hospitals, labs, pharmacies, doctor's offices and health plans.

Data from Connected Health Apps and Devices. Any copy of Health Data from an account you maintain with a third party connected health app or device, which is accessed at your direction through a Health Data Connection.

Data from Suppliers of Digital Health Services. Any copy of Health Data that originates with a third party supplier of digital health services, and is available for you to access and share through a Health Data Connection.

3. Overview of the Purposes of Data Collection

Why does b.well collect Personal Data? Is my Personal Data private?
The b.well application helps you securely centralize your Personal Data from multiple sources so it's all in one place. We also collect that Personal Data to help you make informed health-related decisions, and simplify the process of accessing healthcare services.

The b.well application collects your Personal Data so we can help you build and manage a summary of your health history – sometimes called a Personal Health Record (a "PHR"). Your PHR allows you to see all your Health Data from different sources in one place, manage it and select the Health Data you want to share with others.

We also build personalized insights and tools on top of your Personal Data to deliver more personalized assistance related to your health and healthcare needs. As an example, we can automatically alert you to a care need in need of your attention. Ultimately, our goal with data collection is to give you more ways to conveniently manage your health, and more effectively spend your health dollars.

Because your Personal Data is sensitive, we only collect Personal Data from outside sources with your consent. To learn how, see How b.well Collects Data. We also give you tools to view and manage your Health Data Connections.

4. How b.well Collects Data

How do we collect Personal Data?
We collect data from your use of the b.well application. Also, at your direction, we collect Personal Data through Health Data Connections, which are secure, trusted and private ways for you to give b.well permission to access and share your Health Data with external sources. Health Data Connections are central to our way of helping you create and manage a Personal Health Record.

We collect Personal Data from your use of the b.well application. We also collect Personal Data through "**Health Data Connections"**. Health Data Connections are secure, trusted and private ways for you to give b.well permission to access your Personal Data from external sources for your personal use. In addition, b.well maintains Health Data Connections that allow you to share information with third parties at your direction. The kinds of Personal Data we can collect and share through Health Data Connections includes ePHR Data, Data from Connected Health Apps and Devices, and Data from Suppliers of Digitally Enabled Services. We only collect and share this Health Data with your voluntary, affirmative and informed consent.

By voluntary, we mean that we will not deny your access or use of b.well products or services, including b.well application, if you don't give a consent. If some features or benefits are not available without consent, we explain these limitations so you can make an informed choice. By affirmative, we mean your consent must be indicated by a deliberate act (for example, by clicking an "I Authorize" or "I Accept" button). By informed, we mean that we provide context to help you understand the scope of consent you are granting.

We also support your choice to stop collecting Personal Data from sources outside of b.well. For more information see Data Deletion, Corrections, Retention and Account Changes.

5. How b.well Uses Data

How does b.well use the data collected through the b.well application?
We use your data to help personalize the way you access and use your Health Data, and also to provide more personalized support as you make decisions related to your health.

Your Personal Data allows the b.well application to deliver personal health recommendations and insights through your b.well account. Read Email, Text Messages and Push Notifications to learn more about other methods for communicating with you, and your ability to select communications preferences.

We also use Personal Data to create Non-Personal Data to further our lawful activities, and minimize access to Personal Data in our internal operations.

We use your Personal Data, including your Health Data, to:

- help personalize the way you access and use your Health Data, and also to provide more personalized support as you make decisions related to your health
- operate and improve our b.well products and services
- identify, prioritize, develop, launch and measure the effectiveness of different health programs, tools and benefits that we offer
- help us meet our compliance obligations with regulatory authorities, and meet our contractual commitments to you, based on the terms you have accepted with us
- send you communications
- provide you with customer service and technical support
- evaluate service performance and user behavior
- notify you of new features or service offerings
- notify you of other benefits
- maintain system security and your Personal Data's privacy
- obey laws and help prevent theft, fraud and abuse
- enforce our agreements and policies.
- support purposes that are not listed in this section, but only with your affirmative, voluntary and informed consent

Non-Personal Data. We may use Personal Data to create Non-Personal Data. "Non-Personal Data" means information that does not identify you or members of your family or household personally, and cannot reasonably be used to re-identify you or members of your family or household after it has been removed of individual identifiers. We only use and share Non-Personal Data to support the above business purposes.

A Word of Caution. We appreciate your Personal Data is sensitive. For this reason, we remind you not to share your b.well account username and password with others. If you decide to share these login credentials with someone else, we deem these individuals to be acting with your consent, and you are responsible for their actions, including complying with the Terms.

6. User-Directed Health Data Exchange

How do I decide to share my Personal Data with others?
b.well gives you different ways to share your Personal Data with yourself, b.well and others. The b.well application includes tools that help you view, change and revoke consents.

The b.well application gives you different ways to share your PHR, or parts of it, with other b.well application users or others. We only share this Health Data with your voluntary, affirmative and informed consent, consistent with the consent standards described in How b.well application Collects Data.

The right to share Personal Data includes the right to change your mind. The b.well application includes tools that help you view, change and revoke consents.

Revoking consent is different from deleting data. Read Data Deletion, Corrections, Retention and Account Changes to learn more about data deletion requests.

Deciding to share your Health Data is a personal choice and responsibility. You accept responsibility for decisions to share that Health Data, and for the decisions they make with your Personal Data. You should only share your Personal Data with others that you trust.

7. Disclosures to Others Without Consent

When can data from my b.well account be disclosed to others without my voluntary, affirmative and informed consent?
b.well may need to disclose Personal Data to deliver services, perform its business operations or meet its legal obligations. Here are a few key points:

- *By accepting this Privacy Policy and using the b.well application, you are not giving default consent for b.well to sell or trade in your Personal Data or Non-Personal Data.*
- *We provide specific data privacy commitments to you in case we sell our business, or undergo a corporate restructuring.*
- *If we have a legal or law enforcement request to disclose your Personal Data, we scrutinize these requests, notify you (if we can) and attempt to minimize the Personal Data we must share*
- *We use the third party service providers that are published from time to time on our website under Sub-Processors. We may disclose your Personal Data or Non-Personal Data to them for purposes consistent with How b.well Uses Data. We hold our third party service providers to data protection standards consistent with our own commitments, including the standards set forth in this Privacy Policy.*
- *As we also explain in our Tracking Technologies Policy, b.well does not control the data practices of advertising networks and similar third party technology platforms that track your online activities.*

By accepting this Privacy Policy and using the b.well application, you are not giving default consent for b.well to sell or trade in your Personal Data or Non-Personal Data.

There are limited occasions when b.well has a legitimate business purpose to disclose Personal Data or Non-Personal Data to third parties without your voluntary and affirmative in-app consent. These occasions are described below.

a. Third Party Service Providers
We use a variety of third-party service providers and technology vendors, which may have access to your Personal Data or Non-Personal Data from time to time. We publish a list of current list of these vendors on our website at https://www.icanbwell.com/sub-processors. We review the data protection measures for all of these vendors, and maintain contracts that require them to uphold our own commitments, including the commitments we make in this Privacy Policy.

b. Law Enforcement and Regulatory Authorities
We do not disclose Personal Data to law enforcement or regulatory authorities unless we determine it is necessary to do so under law to comply with a valid court order, subpoena, or search warrant, and our reasonable efforts to limit disclosure to Non-Personal Data are unsuccessful. We attempt to notify you of the disclosure request unless we are prevented from doing so by law. We closely scrutinize all law enforcement and regulatory requests. We attempt to comply by limiting disclosure to Non-Personal Data, or by redacting information so that only the minimum necessary Personal Data is disclosed. We also attempt to receive adequate assurances from the requesting law enforcement or government agency that it will protect the Personal Data to the highest degree possible and will not disclose it in violation of applicable federal or state confidentiality laws. If feasible, we will consider seeking a protective order covering the disclosure. While we cannot offer assurance that any of these efforts will be successful, we will maintain a record of disclosures.

c. Civil Proceedings
If b.well is a party to a legal proceeding with you, we may disclose your Personal Data to the court or arbitrator for purposes of resolving a civil dispute. In doing so, we will sign a qualified protective order, to limit the risk of re-disclosure of your Personal Data. If b.well is not a party to a legal proceeding, we may be required by law to disclose your Personal Data pursuant to a valid subpoena, discovery request or other lawful process. We also will use reasonable best efforts to limit disclosures of Personal Data to the minimum necessary to accomplish their intended purpose.

d. Business Transfers
If we enter into a merger, acquisition, or the sale of all or part of our assets, your Personal Data and any Non-Personal Data will likely be part of the assets transferred. If this happens, we will attempt to notify you, using the e-mail address you have provided in your account profile. We will use commercially reasonable efforts to ensure that the successor entity maintains commitments that are consistent with this Privacy Policy; otherwise, we will disable your b.well account and dispose of your Personal Data before the business transaction is finalized.

e. Advertising Networks, Cross-Device Linking and Do Not Track Signals
Third parties, like advertising networks, web analytics companies and social media and networking platforms, may collect information about your online activities over time and across multiple web and mobile platforms. We are not responsible for third party Tracking Technologies, or for the targeted advertisements they may cause to be served to you on other platforms. We encourage you to check the privacy policies of these third parties, and use browsers, broadband services and devices that you trust when you access and use the b.well application.

8. Email, Text Messages and Push Notifications

How does this Privacy Policy apply to emails, text messages, or in-app notifications?
You may receive communications related to your b.well account via email, text message, or push notification. By default, we only include generalized health information in these communications. If given the option to receive more personalized messages, be aware that these communications are not secure, and they may be visible to others with access to your devices.

By creating a b.well account, you may receive personalized communications via email, text message, and push notifications ("electronic communications"). By default, we only include Account Information (user name, contact information) and generalized health information in these communications. Your b.well account settings give you the option of personalizing your communication preferences. These preferences include giving you choices about the level of personal health-related detail that may be included in these communications.

When selecting these preferences, keep in mind that electronic communications are not necessarily confidential or secure methods of communication. Any Personal Data that you accept through electronic communications may be more readily visible to unwanted and unauthorized parties. For example, they could be intercepted, read by a third party, and/or used for inappropriate purposes. In addition, once an electronic communication is received by you, someone may be able to access or view your screen on your phone, applications, digital devices, or email accounts and read the message. You understand that it is your responsibility to make sure that only authorized people are allowed to access your email, phone messages, cell phone, and digital devices.

When selecting these preferences, you acknowledge your understanding of these risks, give permission to b.well to communicate with you according to your communication preferences, and accept full responsibility for Personal Data disclosures due to your communications preferences.

If you correspond with us by e-mail or text, you should be aware that your transmission might not be secure from access by unauthorized parties. We have no liability for disclosure of your information due to errors or unauthorized acts of third parties during or after transmission.

9. Data Deletion, Corrections and Retention; Account Changes

Can I delete my Personal Data?
You may delete your PHR from the b.well application at any time.

Can I correct my Personal Data?
If you discover an error in your Health Data, contact us for support. We will investigate the error to its source. If the error originates with a third party source over a Health Data Connection, you may be required to request the correction from them directly.

How long can b.well hold on to my data?
We follow an established data retention policy for deleting the Personal Data of dormant accounts after 10 years and closed accounts after 30 days.

How can I close my account?
You can close your b.well account from within the b.well application. We recommend that you download a copy of your PHR before closing your account.

What happens if b.well suspends access, modifies features or closes my Account?
b.well reserves the right to suspend or modify the b.well application, to suspend or modify some of its features, or to suspend or close your account. We reserve the right to deny access or notice if you violate our Terms, if required by law, or if we believe suspension is reasonable to prevent or mitigate harm.

Data Deletion Requests. You can permanently delete your PHR at any time and for any reason without closing your b.well account.

Data Corrections. You can contact Support if you discover an error in your Personal Data. We will investigate to determine if the error occurred in our systems, and make the correction. If we received the error through a Health Data Connection, you may be required to request the correction from the original data source.

Retention. In general, we retain Personal Data and Non-Personal Data in your b.well account for as long as your account is active or as needed to provide you access to b.well application. We delete the Personal Data of permanently disabled (closed) accounts after 30 days.

These data retention policies may be overridden in our sole discretion if we are allowed or required to retain your Personal Data to comply with our legal and contractual obligations, to resolve disputes or to enforce our agreements with you.

10. Information Security

Tell me about b.well information security measures.
Our system of physical, technical, and administrative safeguards are independently reviewed to ensure that they comply with our privacy and security standards. Even so, there is always a risk of data breach, and you accept that risk. We have protocols in place to notify you and help you through next steps if your data is compromised.

We implement reasonable information security measures to safeguard your Personal Data from unauthorized access, disclosure, use, modification and loss. Information security measures include: secure storage, encryption of digital records in transit and at rest, periodic log reviews, and system backups. We regularly review these measures to consider appropriate new technological and other safeguards. Our system of security and privacy controls are periodically evaluated by independent assessors against industry-recognized information security frameworks. We publish certifications to published industry-recognized security frameworks on our website. We maintain a formal training program to ensure our workforce is familiar with common and emergent security and privacy risks, and their responsibilities for safeguarding consumer information and to report concerns to their immediate supervisors. Despite these and other measures, we cannot and do not guarantee that your Personal Data will be absolutely safe. You acknowledge and agree that you create, collect and maintain your Personal Data in the b.well application at your own risk.

If we believe that the security of your Personal Data may have been compromised, we will notify you as required by applicable laws and regulations.

11. Changes to this Privacy Policy

Will this Privacy Policy change?
It may, but if we change it, we will notify you in the b.well application and via email. The notification will include a link to the privacy policy being replaced and a summary of changes. If the changes are significant, we will give you time to consider the changes before they become effective. Your consent to Privacy Policy updates is required to continue using the b.well application. But if you decide not to consent, you can obtain your Health Data before closing your b.well account.

Sometimes, we might supplement this Privacy Policy with an additional notice. This allows us to add conditions for a specific feature in the b.well application without having to change the Privacy Policy. These additional notices may be published under Additional Privacy Notices or under consents linked to your b.well account settings.

We reserve the right to change this Privacy Policy. When we change it, we will notify you based on your communication preferences. These notifications will include a link to the updated Privacy Policy. The updated Privacy Policy will indicate its effective date, and include links (i) to the privacy policy it is replacing and (ii) a summary of changes.

To continue using the b.well application, you will be required to accept the updated Privacy Policy. If we make significant changes (for example, a new use or disclosure of Personal Data that we have already collected and stored, or a purpose of collection or use that is inconsistent with the previous Privacy Policy), we will give you a reasonable amount of time not to exceed 30 days to consider the changes before they become effective. If you do not accept the updated Privacy Policy, you should close your b.well account before the updated Privacy Policy becomes effective.

Sometimes, we might supplement this Privacy Policy with an additional notice. This allows us to add conditions for a specific feature in the b.well application without having to change the Privacy Policy. These additional notices may be published under Additional Privacy Notices. As well, these notices may be part of voluntary, affirmative consents that you make, and are available to you through your b.well account.

12. Marketing to Minors

Can I use the b.well application if I'm under 13 years old?
No, instead, we give parents and legal guardians the ability to create accounts for minors under 13 years old.

We do not knowingly market to or solicit Personal Data from children under the age of 13. We do not knowingly permit anyone under the age of 13 to have their own b.well account. If we obtain actual knowledge that we have collected Personal Data from a user under thirteen (13) years of age without their legal representative's consent, we will use reasonable efforts to refrain from further using such Personal Data, and take steps to disable further use or access in a retrievable form.

13. International Data Transfers

Does b.well transfer my Personal Data outside the U.S.?
We do not transfer your Personal Data to regions outside the U.S., but it may be accessed when you access the b.well application from outside the U.S. You consent to any transfer of Personal Data to the U.S. when you use the b.well application from another country.

The b.well application is hosted in the United States and does not transfer your Personal Data to regions outside the United States. b.well contracts with third-party service providers that may have personnel located outside of the United States, who may access Personal Data.

If you access the b.well application from outside the United States, the laws of the applicable jurisdiction governing data collection and use may differ from United States law. You assume responsibility for these transfers, and consent to the transfer of any Self-Reported Data to the United States for storage and processing to the extent it was originally collected from you when you are located outside the United States.

14. Accessibility

Where can I get more information if I have more questions about my data or b.well's data practices?
If you can't find answers in the Privacy Policy, ask our support team. It might take a couple days at first. We do our best to resolve questions in 30 days or less.

We use editorial content and graphical design to help you understand our data practices in appropriate context within b.well application, and this Privacy Policy can be accessed from our website and b.well application. This Privacy Policy is also available to read in Spanish. If you still have a question, you can ask for further clarification by contacting b.well Support through the b.well application. We do our best to acknowledge your request within 2 days, and respond within 30 days. Responses may be delayed if we cannot verify your identity or your legal authority to receive requested data. If you feel that any of your privacy concerns have not been addressed, please let us know by contacting Support or our Privacy Team(contact information below).

15. Questions and Concerns

If you have a question about the b.well application, including our related data practices, you can use the Support feature within the b.well application to send us an email, or start a chat or phone call during business hours, Monday through Friday (excluding federal holidays). Please allow 1-3 business days for us to acknowledge your request. We will work to promptly resolve your questions or concerns.

Government regulators offer consumer resources as well, including the U.S. Federal Trade Commission (https://consumer.ftc.gov) and the Office of Civil Rights at the U.S. Department of Health and Human Services (https://www.hhs.gov/hipaa/filing-a-complaint/).

Concerns or complaints can also be directed to b.well's Privacy team

By mail:
Privacy Office
b.well Connected Health, Inc.
145 West Ostend Street, Suite 300
Baltimore, MD 21230

Telephone:
443.584.3755

E-mail:
privacy@icanbwell.com

16. Additional Privacy Notices

How will my Device Data be used when I use b.well?
The b.well application will display a prominent disclosure describing the limited purposes and uses for requesting permissions to access Device Data or features on your device. These disclosures are summarized in this supplement, and elsewhere throughout this Privacy Policy. When presented with this disclosure, you will be given a choice to access these permissions. Keep in mind that some functionality may not be available to you should you decide not to accept these permissions.

Google Play Supplement for Android Users –
The Google Play store has determined that the b.well application is subject to Google Play's additional disclosure and consent requirements. As a result, we are required to provide the following information so we can make the b.well application available to you in the Google Play store.

- The b.well application may interact with your device's calendar, camera, photo library and read/write functions of the internal and/or external storage features, but only if you choose to use these device features, for example, to upload documents and media (for example, images, audio or video) files. The b.well application displays prominent in-app disclosures at the time access to these features is requested, about the reasons for accessing these device features. b.well application cannot access these features without your affirmative, voluntary and informed consent.
- By way of example, the b.well application might request access to a digital calendar to store an appointment reminder, access your device's camera or photo library, or temporarily use external storage to edit an image to (i) add a photo to your b.well profile, (ii) add documents to your b.well application digital wallet (for example, your COVID-19 vaccination record, lab test results, or an insurance card) or (iii) verify your identity.

TEFCA Privacy and Security Notice

17. Revision History

November 11, 2025 Revisions
- Overall formatting and language changes
- Removed "Enterprise Sponsors and b.well's ongoing HIPAA responsibilities" and made conforming changes
- Added a reference to a new "Privacy and Security Statement for b.well enterprise customers and their end users"
- Added contact information for submitting concerns or complaints to b.well's Privacy team
- Modified Cookie Policy references to Tracking Technology Policy
- Clarified that Non-Personal Data is not used or shared outside the permitted uses without voluntary, affirmative and informed consent.
- Added a link under Additional Privacy Notices to the Supplemental Privacy and Security Notice (required by TEFCA)

November 2, 2023 Revisions
- Updated the introductory paragraph to make clear that b.well Privacy Policy only applies to b.well-branded applications.

June 7, 2023 Revisions

- Added the Questions or Concerns section.
- Updated the Google Play Supplement for Android Users, explaining the purposes for requesting permissions to access device location services

November 16, 2022 Revisions

- Updated Device Data under Categories of Data We Collect to specify that documents or media (image, audio, video) files may be uploaded by users, using the camera, photo library or read/write internal and/or external storage features of their device, and conforming changes to the Google Play Supplement for Android Users.

September 07, 2022 Revisions

- Removed the COVID-19 Return to Work Supplement from Additional Privacy Notices.

August 9, 2022 Revisions

- Updated §1 Intro`clarify that the b.well Cookie Policy is part of the Privacy Policy, and also updated the Key Takeaway
- Re-ordered the sections, by moving "Enterprise Sponsors and b.well's ongoing HIPAA responsibilities" to §2, to emphasize key data practices and privacy principles
- Updated §3.a (Categories of Data)
- Updated the Key Takeaway to include a prominent disclosure that the application collects sensitive personal information, as required by Google Play policies.
- Clarified that "Non-Personal Data" also refers to data that cannot be reasonably used to re-identify an individual, family or household to the data originally associated with that individual, family or household
- Added Device Data as a sub-category of User Content
- Clarified that User Content may be Health Data or Other Personal Data, and depends on whether Health Data is included in User Content
- Added examples to the chart to reflect the updated Data Category taxonomy, including Device Data
- Added §4 (Overview of the Purposes of Data Collection)
- Updated §5 (How b.well Collects Data)
- Added explanations of how Device Data might be collected by the Application
- Added §7 (User-Directed Health Data Exchange)
- Consolidated disclosures from other sections under this heading
- Disclosures requiring user consent are collected under this heading
- Updated §8 (When b.well May Disclose Data to Others)
- Limited disclosures under this heading to examples when user consent will not be required
- Updated Additional Privacy Notices
- Added Google Play Supplement for Android Users
- Added Digital Identity Supplement