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

b.well

Privacy and Security Statement

Table of Contents

This Privacy and Security Statement describes our minimum privacy and data practice commitments when we collect or process personal information as a technology vendor for our customers.

---

1. Who is b.well?

b.well Connected Health, Inc. (alternately, “b.well”, “we”, “us” or “our”) is a health technology company. Our customers (“customers”) include technology companies and healthcare organizations that integrate one or more b.well products, services and solutions into their consumer-facing applications or services. These integrations help our customers deliver simplified, personalized connected health experiences for their end users (“you” or “your”) under their brands (each, a “digital property”).

When you use a customer’s digital property to create a Personal Health Record (as defined in Why does b.well collect this personal information?), you may be introduced to b.well as their secure data intermediary partner. In this role, b.well will retrieve your personal health information from other sources on your behalf, and transfer it to the customer’s digital property.

As our customers’ service provider, our contractual obligations are not with you, but with our customer. Any personal information we collect, process or transfer on your behalf is governed by their terms of service and privacy notices with you. We are contractually restricted from collecting, using or sharing your personal information, except as described in our customers’ privacy notices or authorized through consents they collect through their digital properties.

2. When does this Privacy and Security Statement apply, or not?

If you are using a b.well-branded digital property (meaning, an online or mobile application that specifically references the b.well Terms of Service), then this Privacy and Security Statement does not apply. Instead, the b.well Privacy Notice applies.

3. What types of personal information do we collect?

Below is a list of different types of personal information we collect:

Personal Information from our Customers. Personal information that we receive from a customer to support its integration with our products, services or solutions. This can include information that links personal information from our services with your customer account.

Passive Data. Information that b.well creates or collects and links with the personal information we maintain to manage our products, services or solutions. This information can include things like tokens, which are technological means for maintaining secure Health Data Connections (defined under How b.well Collects Data)

ePHR Data. Personal information that originates from the medical records that a third party maintains, and makes available to you through Health Data Connections. Examples include information that is maintained about you by specific health systems, health plans, doctor’s offices, pharmacies, and/or clinical laboratories from their systems of record.

Personal Information from Other Third Parties. Personal information that we receive from third parties outside of Health Data Connections. For example, we may integrate with providers of digital identity solutions and suppliers of connected health applications and devices, which allows you to retrieve personal information from your accounts with them.

4. Why does b.well collect this personal information?

We collect this personal information with your consent so our customers can offer you a Personal Health Record (a "**Personal Health Record"** or "**PHR"**) in their digital properties. Having a PHR means you can see all your ePHR Data in one place, instead of having to look up and manage your ePHR Data in different patient portals or consumer-facing applications.

Depending on our contract with a customer, we may offer different kinds of PHR-based capabilities and functionalities. Ultimately, the capabilities and functionalities of our products, services and solutions align to b.well's broader mission to deliver simplified, personalized connected health experiences under our customers' brands, under a consent framework that allows you to exercise meaningful choices in how your Personal Health Record gets used and shared.

5. How b.well collects personal information

The most important way we collect personal information is through Health Data Connections. **"Health Data Connections"** are secure, trusted and private ways for you to access your ePHR Data through b.well, with your consent, for use in your Personal Health Record. Other ways include secure connections with our customers, from sub-processors that we use to deliver our services, and other third parties, as described in What types of personal information do we collect?

6. How b.well uses personal information

To the extent permitted under our customer contract commitments, we use personal information to:

- Facilitate the creation of and secure your account;
- Facilitate your ability to establish Health Data Connections, securely access your ePHR Data, and transfer it to your account;
- Provide, troubleshoot and improve our services. We use your personal information to provide functionality, analyze performance, fix errors, create anonymized and aggregate statistics, and improve the usability and effectiveness of our services;
- Comply with our legal obligations;
- Help prevent theft, fraud and abuse;
- Maintain system security and your personal information's privacy; and
- Support other purposes that are not listed in this section, as long as it is authorized by our customer and consistent with your lawful and valid consent.

7. Does b.well share your personal information?

b.well is restricted by our customer contract commitments from sharing your personal information outside of delivering our services, performing our business operations, or meeting our legal obligations. Here are a couple of key points:

- **Customers.** b.well shares your personal information with the customer whose digital property you are using to access b.well products, services and solutions. The customer's end user terms of service and privacy policy govern our processing of your personal information for this purpose.
- **Health Data Connections.** b.well shares personal information as necessary with other companies and organizations to support your ability to access and exchange personal health information. This includes minimum demographic information for fraud protection.
- **Third party service providers (sub-processors).** b.well contracts with sub-processors to help us deliver our products, services and solutions. b.well publishes a list of these sub-processors at https://www.icanbwell.com/sub-processors/. Some of these sub-processors may have access to your personal information. 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 to our customers.
- **Law enforcement and regulatory authorities.** We do not disclose personal information to law enforcement or regulatory authorities unless we determine it is absolutely necessary to do so to comply with a valid court order, subpoena, or search warrant, and our reasonable efforts to limit disclosure are unsuccessful. We closely scrutinize all law enforcement and regulatory requests. We first attempt to notify our customers of the disclosure request unless we are prevented from doing so by law. If we are prevented from notifying our customers, we attempt to comply by limiting disclosure to anonymized and aggregated statistics. If that is not possible, we then attempt to comply by redacting information so that only the minimum necessary personal information is disclosed. We also attempt to receive adequate assurances from the requesting law enforcement or government agency that it will protect personal information 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.
- **Civil Proceedings.** Civil disputes involving the potential disclosure of your personal information are governed by our contractual obligations to our customers.
- **Business Transfers.** If we enter into a merger, acquisition, or the sale of all or part of our assets, our customer contracts will likely be part of the assets transferred. If this happens, our transfer of your personal information will be governed by our contractual obligations to our customers.

8. How does b.well keep personal information secure?

We implement reasonable information security measures to safeguard personal information from unauthorized access, disclosure, use, modification and loss.

We work to protect the security of personal information during transmission by using encryption protocols and software.

We maintain physical, electronic, and procedural safeguards in connection with the collection, storage, and disclosure of personal information.

Our security procedures mean that we may ask to verify your identity before we disclose personal information to you.

It is important for you to protect against unauthorized access to your login credentials and to your computers, devices, and applications.

When building a Personal Health Record, it is important that you only attempt to collect ePHR Data for yourself, instead of collecting ePHR Data for other people.

While we have safeguards to make personal information available and usable, b.well and our customers do not have full control whether your ePHR Data will be timely, complete or accurate. For example, some external sources may not share any ePHR Data through Health Data Connections. Others may prevent specific kinds of personal health information from being shared through Health Data Connections because it is considered to be especially sensitive. Even when ePHR Data is available, external sources can introduce transmission delays, data formatting errors or errors that originate in their system of record. You should always keep these limitations in mind as you build and use your Personal Health Record. And, always take care not to rely exclusively on your ePHR Data, or use our customers' digital properties as a substitute for appropriate medical care.

9. Your rights

Subject to applicable law, you may have certain rights, but they are exercised through your customer account. b.well supports its customers so they can help you:

- ask whether we hold personal information about you and request copies of this personal information and information about how it is processed;
- request that inaccurate personal information be corrected, or provide information on where to go if your personal information was inaccurate when we received it;
- withdraw consent for the processing of your personal information through our services;
- request deletion of personal information through our services;
- object to the processing of personal information; and
- request portability of personal information that you maintain about you (which does not include information derived from the collected information).

10. Changes to this Privacy and Security Statement

We reserve the right to change this statement, but these changes will not impact our underlying contractual obligations with our customers without their permission.

11. Additional Notices

Some of b.well's products, services and solutions give end users of our customers the ability to retrieve the ePHR Data through trusted exchange frameworks, without having to search for individual data sources. In these instances, our customers are required to present and get individual-level consent to our Supplemental Privacy and Security Statement (required by TEFCA) within their digital property. In these circumstances, the Supplemental Privacy and Security Statement (required by TEFCA) will govern b.well's retrieval of ePHR Data on behalf of a customer's end user, and transfer of that ePHR Data to the customer's digital property.

12. Revision History

First published on November 11, 2025.