MyCareWare Privacy Policy

Last Update: August 1, 2020

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

MyCareWare develops health care technology or apps that collect digital health data about individuals that may be accessed and used by the individual and the individual’s health care providers.

MyCareWare’s primary customers are health care professionals (“Customers”) who perform healthcare risk assessments and access our database of the testing results that can be downloaded or accessed via a proprietary network on the internet or via the practice’s electronic health record system.

This document is intended to disclose to consumers (“Patients”), our privacy and security policy. “We” refers to MyCareWare and its technology products and services, and “you/your” refers to the consumers/patients whose information may be stored in our health technology platform.

MyCareWare, Inc is a HIPAA-covered entity, because the data we collect and protect, is considered identifiable Personal Health Information (“PHI”). For more information about HIPAA regulations and your rights, please visit <https://www.hhs.gov/hipaa/index.html>.

We collect, use and may share your PHI with companies or entities to:

* Provide the primary services of our technology
* Conduct scientific research
* Support company and physician practice operations
* Develop and improve new and current products and services

We share your data AFTER removing identifiers (note that remaining data may not be anonymous) when we believe that the identifiers are not necessary in carrying out any task for which the data may be used.

We do not sell your data to: data brokers, marketing firms, or advertising firms.

Your data is not stored on any local device (like a tablet or laptop computer) at our company.

Once your data enters our application, it is automatically encrypted, both while “at rest” (stored and not in use) and while “in motion” (moving between apps or systems.)

With your permission, our technology may request access to other device data or applications, such as your phone’s camera, location services, health monitoring devices, contacts, photos, microphones, or commercial fitness applications like Fitbit. You have the right to decline this request.

With your permission, our technology may allow you to share the collected data with your social media accounts, like Facebook.

Because the data we collect may be used to audit compliance with certain regulations, and/or may be accessed for legal proceedings, you may not delete the data we collect. We are also contractually committed to maintain this auditable data for up to 25 years, or at least 7 years after your last interaction with our technology. You have the right to get copies of the data, which will be made available in file form, which you can download from our secure portal. Analysis conducted using your data may not be available to you. You will have access to the data we collect from you and your health care providers through our consumer/patient portal.

If our privacy policy changes, we will notify you via email, text and/or mail, based on the contact information we have on file. Mail will only be sent to those customers/patients who have no email or text on file, and whose records have been accessed by the consumer/patient or the practice, within the last 7 years.

MyCareWare complies with all applicable laws regarding breaches. Should we have a breach of your data, you will be notified by email, text, and/or mail. At that time, we will advise you of actions you may take, as well as the actions we are taking to identify and remediate the cause of the breach.

Should you have questions or feedback regarding any information contained in this policy, please contact us using the “Get In Touch” button on this site.

page5image8957952

Health data can include but is not limited to: wellness information (e.g., exercise or fitness habits, nutrition, or sleep data), health markers (e.g., blood pressure, BMI, or glucose), information on physical or mental health conditions, insurance or health care information, or information that integrates into or receives information from a personal health record.

Identifiable data means: data, such as your name, phone number, email, address, health services, information on your physical or mental health conditions, or your social security number, that can be used on its own or with other information to identify you.

Analytics means: the process of examining data to draw conclusions from that information.

Data broker means: companies that collect personal information about consumers from a variety of public and non-public sources and resell the information to other companies

Encryption means: a method of converting an original message of regular text into encoded text in such a way that only authorized parties can read it.

Cloud computing provides shared processing resources and data to computers and other devices on demand.

Deactivation means: an individual takes action or a company ceases operation or deactivates an individual’s account due to inactivity.

Breach means: an unauthorized disclosure.