# **Way to Health Summary of Data Protections**

# Introduction and purpose

This document outlines how protected health information (PHI) is stored, secured, and accessed on Way to Health (W2H). For a complete list of data protections and associated policies and procedures, please visit <https://policy.waytohealth.org>.

## What is W2H?

W2H is a web-based platform that provides sustainable technology infrastructure for conducting behavioral economic research studies and automated hovering and remote monitoring clinical programs. The platform's flexible design and focus on automation enable users to deploy tailored interventions for specific patient populations anywhere in the U.S. with minimal effort at low cost. And when successful interventions are identified, W2H supports implementation in clinical settings so that health benefits can be realized over time.

Features of the platform include mobile participant enrollment; survey administration; integrated biomedical device data transmissions; automated randomization in a variety of schemes; automated communication with participants via voice, text, and email; delivery of financial and social incentives; utilization of gamification strategies, and much more.

W2H is operated through a partnership between the Penn Center for Health Incentives and Behavioral Economics (CHIBE) and the Penn Medicine Center for Health Care Innovation. More details are available at <https://healthcareinnovation.upenn.edu/way-health>.

# How PHI is stored on the platform

W2H can collect multiple pieces of data from patients and participants per study requirements. This includes personally identifiable information (PII) such as name and date of birth and health information such as diagnosis or medications. This information can be requested and collected via secure, customized surveys or direct integration with electronic health records (EHRs).

# Access controls

W2H uses a role-based access control (RBAC) approach to assure that participant confidentially and study integrity are preserved. Access and visibility are primarily governed by the role of the individual accessing the system. Access is granted by invitation only and can be revoked at any time. More details are available here - <https://policy.waytohealth.org/#7-system-access-policy>.

**Research personnel**: This includes roles such as principal investigators, project managers, research coordinators, and statisticians. Staff such as principle investigators and statisticians are restricted using RBAC, with a role that provides them access to de-identified data sets only. Other staff, such as project managers and research coordinators, require access to identifiable data in order to conduct normal study operations such as follow-up study visits, monitoring enrollment statuses, and updating contact information. These roles can toggle between identified and de-identified views as needed. Prior to receiving access to the platform, the study’s project manager must confirm that the staff person has been added to the IRB and has completed their CITI Protection of Human Subjects Research Training – ORA. Research staff users must read and sign the W2H Data Security Agreement upon initial login to the platform. They cannot access PHI or any other data on the platform until that agreement has been reviewed and signed.

**W2H personnel**: The W2H team supports all research studies run on the platform. Default views within the platform for all W2H staff display de-identified participant data. As a part of support and troubleshooting, the W2H team is trained to use only these de-identified views. In rare cases where an issue involves viewing identifiable participant data, members of the W2H team may need to view data to assist the study team. W2H staff are employees of the University of Pennsylvania and Penn Medicine. All W2H team members have completed HIPAA Security training and CITI Protection of Human Subjects Research Training - ORA. Access to the backend database is restricted and only available to a select group of developers. The database is accessible only via a secure virtual private network (VPN) and cannot be accessed from the public internet at all, i.e., authorized users can only access the databases from within Penn’s network and over a secure VPN channel.

# Data integrity controls

To maximize security, W2H assumes that **all** data in the system is electronic protected health information (ePHI). Details of controls in place are available at <https://policy.waytohealth.org/#17-data-integrity-policy> and are summarized below.

#### Server environments

All W2H servers are managed by Penn Medicine Academic Compute Services (PMACS).

#### Encryption at-rest

All data at-rest is stored on encrypted disks using encryption keys managed by W2H. Encrypted disks use AES encryption with a minimum of 256-bit keys, or keys and ciphers of equivalent or higher cryptographic strength. User passwords are never stored in clear text; they are “salted” and “hashed” to eliminate data leakage.

#### Encryption in-transit

All data transmission is encrypted end to end using encryption keys managed by W2H. Transmission encryption keys use a minimum of 2048-bit RSA keys or keys and ciphers of equivalent or higher cryptographic strength (e.g., 256-bit AES session keys in the case of IPsec encryption).

Data downloads are generally prohibited by policy. Where appropriate, most datasets are blinded of all personally identifiable information when exported for analysis. A limited number of exports, including identifiers, exist to assist research staff with recruitment tracking and study management efforts. These datasets are only accessible to certain user roles. These user roles are required to sign and adhere to a W2H Security Agreement as described above.

#### Audit logging and monitoring

To monitor ongoing usage of the system and identify unauthorized usage of the system, all access to the application and the database are logged automatically. These logs are reviewed as described in the W2H policies.

# Data loss prevention controls

The intent here is to minimize data loss. This is done through the policies and procedures detailed here – Data Management Policy (<https://policy.waytohealth.org/#6-data-management-policy>), Disaster Recovery Policy (<https://policy.waytohealth.org/#13-disaster-recovery-policy>), Intrusion Detection Policy (<https://policy.waytohealth.org/#15-ids-policy>), and Vulnerability Scanning Policy (<https://policy.waytohealth.org/#16-vulnerability-scanning-policy>). This is summarized below.

Backups

W2H has automated procedures to create and maintain retrievable exact copies of ePHI utilizing our Backup Service. These backup procedures are run daily and stored in different locations. Backups are encrypted. Backups are retained for a rolling 14-day period. Recovery from backups is also tested on a quarterly basis.

Disaster recovery

W2H has policies and procedures in place for system recovery following a disruption resulting from a disaster (such as extended outages).

Security scanning

Security is a paramount concern at W2H. We perform regular (at least monthly) vulnerability scans of our systems to identify and patch any known vulnerabilities in our systems. We also run Intrusion Detection Systems (IDS) to identify unauthorized system access.

# Communication with human subjects

Individuals are asked to provide their name, email address (personal or work), and phone number for the duration of the study. Participants are given the choice to receive automated study notifications and alerts via email, text message, phone, or any combination of the above.

# W2H links to external applications

The use of W2H includes access to an ecosystem of devices and web applications. This enables study teams to collect data such as steps, weight, blood pressure, and patient-reported outcomes. This data is paired with frequent behavioral feedback provided to the participant. For example, in a weight loss study, the research team might establish daily or weekly weight goals for a participant, interface with an Internet-connected scale, and award the participant 10 points each day they weigh in and 100 points if they meet their weekly weight loss goal.

W2H has integrations with a variety of biometric and other devices (e.g., pedometers, scales, electronic pill bottles), communication services for sending/receiving SMS/MMS/IVR, communication services for sending email, Qualtrics for surveying, and Penn Medicine’s EHR, Epic.

Data flows

There are three primary data flows we use for device integrations: 1) consumer-authenticated devices, 2) researcher-managed devices with API querying, and 3) researcher-managed devices with data push. All three flows involve the physical devices connected to and communicating with a vendor-managed server. The mechanism for how the data gets from the vendor server to W2H, and the authentication mechanism used for that connection, differ between the three flows.

##### Consumer-authenticated device

*Examples: Fitbit, Withings*

For a consumer-authenticated device, the participant will create an account with the device vendor, link their device to the account (frequently setting up the device via Bluetooth), and then authorize W2H to access their data using a mechanism such as OAuth. For a research study, devices will frequently be purchased by the study and provided to the participants, but the account on the vendor system will belong to the participant rather than to the research team.

Once the participant’s account is authenticated to W2H, we have an hourly background job that queries the vendor API for activity since the last data point that was downloaded, using an API endpoint like “show all activity since Y/M/D.”

##### Researcher-managed devices with API queries

*Examples: Adheretech, Wisepill*

In the researcher-managed device flows, the participant does not interact with or create an account on the vendor portal. Instead, the researcher has an account where they can view devices purchased, possibly register or set up devices, and see activity from the devices. Typically, these devices communicate with the vendor portal through a cellular connection (sometimes through an intermediate hub) rather than through a participant’s smartphone and Bluetooth. Once the device is configured on the vendor portal, the researcher will enter a device ID (e.g., a serial number, MAC address, or other ID) into the participant’s profile in W2H. W2H will then do an hourly query for activity since the last downloaded data point.

##### Researcher-managed devices with data push

*Example: Qualcomm 2net SP*

In this flow, like the previous researcher-managed device flow, the device is configured by the research team in the vendor portal. However, rather than an hourly process where W2H pulls data from the vendor server, instead, the vendor server pushes data to W2H as it is processed from the device or hub.

## Qualtrics

Prior to having our own survey builder, study teams exclusively used our Qualtrics integration to manage survey administration. This feature is only being used for studies started on the platform before March 2018. Survey answers are stored on the Qualtrics server before we retrieve them and save them on the platform. All interactions between a participant and the Qualtrics server are de-identified. Study staff members review the survey content to ensure that no questions in any of the surveys ask for patient identifiers. To ensure no patient-identifiable data is stored by Qualtrics, we use randomly generated 64-bit identifiers to link responses in Qualtrics to study events in our system. No PHI will ever be stored by our application in Qualtrics.

## Communication vendors

Most studies built on the platform employ some form of notifying participants and research coordinators either by text message, IVR or email. For text messaging and IVR, W2H uses Twilio Cloud Communications ([http://twilio.com](http://twilio.com/)). While Twilio logs the content of each message that passes through its system along with the phone number, W2H automatically deletes the content of the messages from Twilio continuously. This allows W2H to collect health information such as patient-reported blood pressure readings.

We use Sendgrid (<https://sendgrid.com/>) for all email communications. W2H fully recognizes that emails are not a secure communication channel. Thus, emails auto generated by W2H do not contain ePHI. This is also communicated to study leads and project managers.

## EHR

W2H is integrated with Penn Medicine’s HER, Epic. W2H can link a participant profile with a patient’s chart in Epic using the patient’s MRN. W2H allows the user to configure additional fields for validation such as name, address, and phone number.

Using this integration, W2H can retrieve study relevant data from Epic, primarily appointment data. Appointment dates can be used to trigger actions in the W2H intervention such as starting a participant after surgery or sending a reminder of an upcoming appointment. W2H also has the capability to send data sets collected on the platform into Epic flowsheets. These data sets are reviewed and pushed over by clinicians who have access to W2H.