**Way to Health Platform**

**Summary of Data Protections**

1. **What types of PHI are collected through the Way to Health (WTH) Platform and who would have access to the PHI?**

Way to Health collects subjects’ names, date of births, addresses, email addresses, phone numbers, and social security numbers. We also request the name and phone number of an alternate contact. Depending on the type of study, we may also collect medical record numbers and computer IP addresses. To assure that participant confidentiality is preserved, individual identifiers are stored in a single password protected system that is accessible only to study research, analysis and IT staff. An investigator or statistician who logs in will be able to access only de-identified data. The Way to Health administrative group and research coordinators responsible for contacting participants for follow-up study visits or responding to questions about the study are able to view participant names and contact information. The WTH web development team and Project Director currently have administrative access to PHI. All of these personnel will have completed Human Subjects Protection and HIPAA privacy training. The system automatically generates logs of all data queries which can be reviewed by research staff to ensure that no unauthorized persons have gained access to identifiable information. This system is hosted on site at The University of Pennsylvania (UPenn) and is protected by a secure firewall and several layers of operational security. Once a participant has been entered into this system, they are given a unique study identification number (ID). Any datasets and computer files that leave the firewall are stripped of all identifiers and individuals are referred to by their study ID. The study ID is also used on all analytical files.

1. **How will data be encrypted and shared across systems (e.g. Withings to Way to Health)?**

The Penn Medicine Academic Computing Services (PMACS) is the hub for the hardware and database infrastructure that supports the project and the Way to Health web portal is built on this infrastructure. The data collected for Way to Health based studies is stored in mySQL databases on a PMACS-operated blade server environment devoted specifically to Way to Health. The data center is housed in Information Systems and Computing at 3401 Walnut Street. All data are stored in a single relational database, allowing researchers to correct mistakes. Every SQL transaction, including accessing and changing data, is logged for auditing purposes. Data are entered into the database through several different mechanisms. Participants enter their own personal information and respond to surveys through a PHP-based web interface. Researchers have a separate interface that allows them to manually enter data if needed. Data from biometric/ monitoring devices are uploaded automatically. Datasets are blinded of all personally identifiable information when exported for analysis. The web application automatically removes all identifiers when a researcher requests an analytic dataset. The only people with access to identifiable participant information are pre-specified Research Coordinators responsible for contacting participants for follow-up. Personal information and research data will be stored in separate SQL tables and will be linked by a computer-generated ID number. Additionally, any information that leaves this system to communicate with third party data sources (biometrics devices, survey software, etc.) is stripped of any identifiers and transmitted in encrypted format. The same unique study ID is used to link these outside data to the participants.

For example, participant’s MedApps devices report data to the secure MedApps sever through a transmission device called the HealthPal. The research coordinator registers all participants in the secure MedApps HealthCom system using their name, gender and HealthPal serial number. Their MedApps device serial number will link the HealthCom system with the study platform. Way to Health web developers have built an application that securely and automatically transmits data from the MedApps server to the Way to Health study server. All of the data is encrypted via https and transmitted from MedApps to the Way to Health web application and secure Penn servers. Upon using the devices, participants’ measurements are sent automatically through a secure connection to the study website. Similar interfaces have been built with other device manufacturers.

1. **How will financial information be collected/protected (including SSN for payment of earnings, as well as credit card numbers for payments from subjects to Penn)?**

Social security numbers and back account numbers for all participants to whom payments are sent are transmitted in encrypted format to UPenn’s Financial Systems/Comptroller’s Department where data are stored for compliance with W-9 form reporting requirements. Participant deposits (if applicable by study design) are processed using credit/debit cards handled by Cybersource. Cybersource is a credit card processing company that is PCI (payment card industry) secure. All credit/debit card information will only be handled by Cybersource’s secure servers. In order to minimize the risk of accidental disclosure, social security numbers will only be used to generate W-9 forms and will be deleted once they are no longer needed.

1. **How is survey data entered into the Way to Health platform protected?**

The Penn Medicine Academic Computing Services (PMACS) is the hub for the hardware and database infrastructure that supports the project and Way to Health web portal is built on this infrastructure. Study data are stored in mySQL databases on a PMACS-operated blade server environment devoted specifically to the Way to Health. All data are stored in a single relational database, allowing researchers to correct mistakes. Every SQL transaction, including accessing and changing data, is logged for auditing purposes. Data will be entered into the database through several different mechanisms. Participants will enter their own personal information and respond to surveys through a PHP-based web interface. Researchers have a separate interface that will allow them to manually enter data if needed. Data from monitoring devices will be uploaded automatically. The dataset will be blinded of all personally identifiable information when exported for analysis. The web application automatically removes all identifiers when a researcher requests an analytic dataset. The only people with access to identifiable participant information are pre-specified Research Coordinators responsible for contacting participants for follow-up. Personal information and research data will be stored in separate SQL tables and will be linked by a computer-generated ID number. All data for this project will be stored on the secure/firewalled servers of the PMACS Data Center, in data files that will be protected by multiple password layers. These data servers are maintained in a guarded facility behind several locked doors, with very limited physical access rights. They are also cyber-protected by extensive firewalls and multiple layers of communication encryption. Electronic access rights are carefully controlled by UPenn system managers. We use highly secure methods of data encryption for all transactions involving participant's financial information using a level of security comparable to what is used in commercial financial transactions. We believe this multi-layer system of data security, identical to the system protecting the University of Pennsylvania Health Systems medical records, greatly minimizes the risk of loss of privacy. All communications between users and our site will be encrypted with SSL/HTTPs technology.

1. **How is information about the study communicated to subjects (e.g. would work email addresses be used or only personal accounts)?**

Individuals are asked to provide their name, an 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

1. **What identifiable information is contained in the messages subjects receive about the study?**

Automated study-related emails do not contain identifiable information about a participant or information regarding a participant’s progress in the study. Instead, these automated messages direct participants to log into the secure study website where they will be able to access this information. These messages are also in place to remind participants to complete a pre-specified study task such as a survey completion, device upload, etc.

1. **What personal identifying information is captured by external systems and how is that information protected when stored within those systems?**

Personal identifying information such as name, gender, email addresses, username, password, and health information could potentially be captured by external systems. Way to Health requires all external systems to provide individual security documents clarifying how protected health information will be stored and protected. For example, data collected by the IncentaHEALTH kiosk is encrypted with a private AES-256 bit encryption key immediately following user data entry into the system. The encrypted data is sent via a secure HTTPS/SSL channel to the IncentaHEALTH datacenter. Once at the datacenter, data is stored only as AES-256 bit encrypted values in the database. The datacenter resides behind dedicated Cisco/SonicWall firewalls. The datacenter facility is an ISO 9001:2000-certified provider and is monitored 24x7 by onsite Network Operations Center staff. The physical location of the production servers is behind fully-enclosed locked steel mesh cage housing. Only authorized employees are provided access to sensitive information on an as-needed basis. All data access is performed through the same encrypted communication channels to ensure privacy during information handling. Additionally, a Business Associate Agreement is executed when directed by University and School of Medicine Privacy Officers

1. **What support systems are in place to deal with malfunctioning external devices?**

In the event of a device malfunction, study coordinators notify the Way to Health web developers to ensure that it is indeed a device malfunction and not a website issue. Way to Health web developers and/or Research Coordinators contact designated IT personnel for the respective device to trouble shoot and resolve the issue.