## Database Security/Protection against Risk. To assure that patient, physician and other informant confidentiality is preserved, individual identifiers (such as name and medical record number/physician billing identifier) are stored in a single password protected system that is accessible only to study research, analysis and IT staff. This system is hosted on site at The University of Pennsylvania (UPenn) and is protected by a secure firewall. Once a participant is in this system, they will be given a unique study identification number (ID). Any datasets and computer files that leave the firewall will be stripped of all identifiers and individuals will be referred to by their study ID. The study ID will also be used on all analytical files.

## Additionally, any information that leaves this system to communicate with third party data sources (biometrics devices, survey software, etc.) will be stripped of any identifiers and transmitted in encrypted format. The same unique study ID will be used to link these outside data to the participants.

## Social security numbers, bank account and routing numbers for all participants to whom payments are sent will also be transmitted in encrypted format to UPenn’s Financial Systems/Comptroller’s Department where data will be stored for compliance with W-9 form reporting requirements. After the social security numbers are no longer needed they will be deleted from our system.

The Way to Health (WTH) Research Data Center staff is responsible for preventing unauthorized access to the trial participant tracking system database. It is important to note that the Way to Health database server and individual study databases have never been compromised as a result of the extremely rigorous and secure network firewall technologies. The secure servers are located in a specially designed, highly secured facility at UPenn with dedicated uninterrupted power supply and strictly limited access. The study will utilize a client-server deployed Data Management System (DMS) rather than a 'Store and Forward' database configuration, obviating research site database security concerns. Confidential participant information will be entered into the database. If this information exists on paper CRFs, it will be filed under lock and key, with generation of a participant ID. Thereafter, confidential information will be made available to authorized users only as specifically needed. No one can gain access to an individual MySQL database table unless explicitly granted a user ID, password, and specific access. Even those with user names and passwords cannot gain access to the tables that contain the identifying participant information.

No results will be reported in a personally identifiable manner. All tracking system data will be password-protected with several levels of protection. The first will allow access to the operating system of the computer. The second will allow access to the basic menus of the integrated system; within certain menu options, such as database browsing, a third password will be required. Our prior research employing similar precautions has demonstrated that these techniques are very successful in assuring the protection of subjects.

The same procedure used for the analysis of automated data sources to ensure protection of patient information will be used for the survey data, in that patient identifiers will be used only for linkage purposes or to contact patients. The study identification number, and not other identifying information, will be used on all data collection instruments. All study staff will be reminded to appreciate the confidential nature of the data collected and contained in these databases.

Each investigator and staff member involved in the proposed study will sign and adhere to a Standard Operating Procedure for managing participant data through the WTH platform and has participated in required IRB/HIPAA compliance training. We will also continue to make use of password protection programs for all computerized records. In no instances will identifying information be publicly disclosed. Prior to conducting any analyses, all identifiers (e.g., names, medical record numbers, health plan enrollee numbers, birth dates, etc.) will be removed. Results from this part of the investigation will be reported in aggregate.