March 2014

PHR Ignite—Action

HealthInsight Final Report Assessing the Current Environment and Functionalities of PHR Systems

Prepared for

Office of the National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
300 C Street SW
Washington, DC 20201

Prepared by

HealthInsight, Utah
HealthInsight, New Mexico
Utah Department of Health
Utah Health Information Network

For

RTI International
3040 Cornwallis Road
Research Triangle Park, NC 27709

RTI Project Number 0212050.007.000.500.010

RTI INTERNATIONAL

RTI Project Number
0212050.007.000.500.010

PHR Ignite—Action

HealthInsight Final Report Assessing the Current Environment and Functionalities of PHR Systems

March 2014

Prepared for

Office of the National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
300 C Street SW
Washington, DC 20201

Prepared by

HealthInsight, Utah
HealthInsight, New Mexico
Utah Department of Health
Utah Health Information Network

For

RTI International
3040 Cornwallis Road
Research Triangle Park, NC 27709

Contributing Authors

HealthInsight Utah:
Korey Capozza, MPH
Consumer Engagement Director

Deepthi Rajeev, PhD
Medical Informaticist

Clare Lence
Project Coordinator

HealthInsight New Mexico:
Alex Bradford, MBA
HIT Project Manager

Margy Weinbar
VP Operations

Utah Department of Health (UDOH):
Francesca Lanier
Director, Office of Data Security

Utah Health Information Network (UHIN):
Doreen Espinoza
Chief Business Development and Privacy Officer

RTI International:
Shellery Cunningham
Health IT Scientist
Consortium Project Manager

Stephanie Rizk
Manager, Health IT Policy
SHPC Consortium Task Lead

Robert Bailey
Senior Manager, Health IT Policy
SHPC Project Director

Contents

[This page intentionally left blank.]

1. EXECUTIVE SUMMARY

This project, completed by an eight-person, two-state team, consisted of a comprehensive assessment of the climate for personal health record (PHR) adoption in New Mexico and Utah. It included a review of published literature and an assessment of stakeholder attitudes and opinions in the region. This exercise yielded several important findings that are summarized in this report and reflected in the recommendations. Overall, the research identified key areas instrumental to advancing provider, payor, and patient adoption of PHR technology. The recommendations seek to provide guidance on how to address these key areas.

Privacy and Security

Clarification is needed on the privacy and security provisions of PHRs. A common criterion, similar to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Notice of Privacy Practices, is needed so that all PHRs, especially those that are not covered as business associates of HIPAA-covered entities, may be independently rated. Additionally, simplified user agreements that explicitly state, in plain language, how and when a vendor may use consumer protected health information are needed. Both of these advancements may promote consumer awareness of and trust in PHRs.

Standards

For PHRs to seamlessly integrate with other data sources, vendors need to work toward standardized messaging and exchanges. Health information exchanges (HIEs) play an integral role in exchanging data and managing records from disparate systems and providers of care. Leveraging this infrastructure to bring data into patient records from untethered PHRs (not directly connected to an electronic health record [EHR] system) and payor PHRs holds tremendous promise. Likewise, developing interface connections between tethered PHRs (tied to an individual EHR) and outside sources of clinical data could create more complete patient records and speed adoption of patient-mediated exchange.

Consumer Adoption

Health care providers and consumer advocates are in a position to dramatically increase awareness of PHRs, but in many cases, awareness alone will not suffice to speed adoption. Consumers will need help with signing up and ongoing technology support. Tech-savvy caregivers and parents of children with serious health problems may be effective early adopters and could be a focus of future, targeted adoption efforts. Providers can also encourage use by selecting a user-friendly PHR and implementing features that have clear utility for consumers such as secure messaging, appointment scheduling, and the ability to view laboratory results. Providers must also reassure consumers about the security of their

data, after taking steps to determine that data are indeed both technologically secure and protected.

Bidirectional Data Flow

Providers are cautious to integrate information edited by patients into EHRs and use this information to inform clinical decisions. Patients, on the other hand, have varied opinions on the need to update their health care information. These insights indicate the need for research that explores the value of bidirectional information exchange from the perspectives of providers and patients. Establishing rules and guidelines for the provenance of patient-generated or patient-entered data will be important to ease provider concerns about data accuracy and liability issues.

Implementation

Health care facilities reported several key factors for success in getting providers and patients to use tethered PHRs: (1) making significant workflow changes, (2) training office staff, (3) supporting features desired by patients and providers, and (4) advertising and active patient enrollment. Untethered PHRs not connected to a specific EHR system have limited utility because the onus of populating and maintaining the information is typically on the patient. However, information flow between untethered and tethered PHRs could result in a more convenient and complete patient health care record.

Cost and Incentives

Federal programs currently drive EHR and PHR adoption. Providers and patients must see clear value for the sustained use of PHR technology to continue after these programs end. Understanding and sharing the benefits for providers will be essential if PHR use and adoption are to occur beyond the scope of these incentive and penalty programs. Furthermore, providers will need a revenue stream to offset the time spent supporting and communicating via PHR technology. Future payment models (such as accountable care) may provide an avenue for offsetting the costs currently associated with these tasks.

2. INTRODUCTION

The purpose of this final report is to highlight key findings from the 9-month inquiry into the barriers to and opportunities for broader PHR adoption in New Mexico and Utah. In the first phase of the PHR Ignite project, the two-state team reviewed secondary resources to assess and summarize the published literature on key aspects of the PHR landscape both nationally and locally, in Utah and New Mexico. During the environmental scan, the project team identified information gaps in the published literature. Next, these findings were supplemented with primary sources: discussions were conducted with dozens of key stakeholders in both states to better understand the barriers and opportunities for PHR adoption in the region.

An implementation pilot was conducted to demonstrate bidirectional exchange of data at the primary care clinic level. This pilot explored the concrete steps required, for both clinics and patients, to create a patient-mediated PHR that could receive data from a provider and send biometric data back to the provider's EHR. In this report, the work to date is synthesized and results are highlighted. Finally, the report offers recommendations on policy changes and areas for future research, and identifies potential next steps.

Consumers and providers are taking on new roles as partners in care as the familiar "physician as authority" paradigm gradually becomes obsolete. In the changing health care environment, patients are increasingly involved and engaged in their own health care—a role that they are assuming, at times, somewhat reluctantly. Providers are now required to share more information to help empower patients and facilitate consumer engagement in care. As evidenced by discussions with stakeholders, these changes can cause anxiety for both providers and patients as their traditional roles evolve. As providers and patients adjust to the changing health care landscape, attitudes toward PHRs continue to evolve.

[This page intentionally left blank.]

3. KEY FINDINGS

The three-stage assessment yielded the following key findings from five topical areas: 1) privacy, security and confidentiality 2) interoperability 3) implementation 4) consumer adoption 5) data control. These topics are described in detail below.

3.1 Privacy, Security, and Confidentiality

3.1.1 Increase Awareness, Build Trust, and Promote Broad Use of PHRs

Consumers see value in a more complete and accurate medical record that is portable and secure. However, consumers and providers are apprehensive and skeptical about the security of untethered PHRs. Distrust is fed by a lack of consistent privacy and security standards across the PHR market. In addition, providers rely on validated information for the provision of care and are leery of relying on patient-entered data. Providers are hesitant to allow patients additional editing rights beyond those regularly provided by a patient during an office visit. Many consumers are interested in exerting more control over their medical information; a PHR's capacity to integrate disparate records enables patient control over access and allows tracking of annotated and sourced information.

3.1.2 Lack of Common Language and Definitions

The Health Information Technology for Economic and Clinical Health (HITECH) Act defines a PHR as "an electronic record of PHR identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual."[1] More than 100 PHRs and 750 EHRs with varying degrees of PHR functionality are available on the U.S. market.[2] Although all PHRs store health information, only some PHRs are obligated to meet the requirements of the HIPAA Privacy Rule due to their relationship with HIPAA-covered entities through a business associate agreement (BAA). Other PHRs may operate without being obligated to follow the HIPAA Privacy Rule because they are not bound to a covered entity through a BAA. Although they may provide privacy and security of health information at the same level as a HIPAA-covered PHR, the distinctions can lead to operational differences that affect consumers' understanding of how their data are used. For example, PHRs that are HIPAA-covered are required to store health information under the definition of protected health information (PHI), which is all individually identifiable health information. PHRs that are non-HIPAA-covered may use the term PHI to mean personal health information, a more general term unrelated to the HIPAA

[1] The term "PHR identifiable health information" means individually identifiable health information, as defined in section 1171(6) of the Social Security Act (42 U.S.C. 1320d(6)), and includes, with respect to an individual, information—(A) that is provided by or on behalf of the individual; and (B) that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

[2] Michael Bass Group (2012, January). *Special report—Patent valuation repor*t. Available at: http://www.michaelbass.com/PDF/JAN20MMRF.pdf. Accessed July 30, 2013.

Privacy Rule. Although use of the term PHI by non-HIPAA-covered PHRs is not intended to deceive the consumer, its use may create a false sense of understanding about PHRs and the protections afforded the health information they contain. The consumer must decipher the nuanced differences in how their data may be treated when a PHR is "protected" or governed by HIPAA and when it is not.

3.1.3 Need for Common Privacy and Security Criteria for PHRs to Explain How and When a Vendor May Use Consumer PHI

Few consumers understand the distinction of HIPAA-covered PHRs compared to those not covered, which may contribute to a general sense of distrust reported around PHR systems. HIPAA provides a standard criterion, Notice of Privacy Practices, to describe ways in which a covered entity or its associate may use the consumer's PHI. PHR vendors (and their systems) not governed by the HIPAA Privacy and Security Rules are held to no other federal standard for safeguarding consumers. The consumer using a non-HIPAA-covered PHR must rely on the protections declared in the vendor use agreement and privacy policy, which vary significantly across the PHR market. The consumer bears considerable responsibility to comprehend complex vendor use agreements that use abstruse legal jargon. There is a need to have common privacy and security criteria for PHRs that can simplify vendor use agreements and privacy policies that use plain language, making the material easily understood by the general consumer.

3.1.4 Balancing Consumer Empowerment with Improved Health Care Outcomes

Consumers and providers have vested interests in accurate and accessible medical information. Doubts about the accuracy of provider records and privacy concerns drive growing consumer interest in editing medical record information, controlling who has access to specific information, and having the ability to suppress or limit information from their care providers. PHRs provide consumers some control. However, restricting health information from care providers involved in the treatment of a patient may have unintended and potentially fatal consequences. Stakeholders support consumer engagement and increased involvement in their medical care, but this must be balanced with providers' needs for accurate and timely information.

3.2 Interoperability

3.2.1 Standards Needed

Meaningful Use Stage 2 (MU2) has helped drive EHR vendors to supply a tethered PHR product, which for the purposes of this report is defined as a PHR or portal application associated with a health care provider using a particular EHR system. These PHRs have a clear method for exchanging standardized messages with the EHR to which they are connected and are eligible to become certified for this functionality. In contrast, non-

tethered or standalone PHRs are defined for this report as those not directly tied to an EHR system. Although this lack of a direct tie allows them to avoid a silo, they may not have the ability to send and receive clinical messages in a standardized way. Therefore, few options are available to automatically populate these applications with clinical data.

Untethered PHRs frequently rely upon hand entry as a method to input data, which is a concern for providers if clinical data are included. Providers more readily accept clinical data, such as lab results and medical findings, when they know that the source is a certified clinical system (as opposed to hand entry).

In addition to the challenges of standard messaging described above, the lack of clinical data standards is a persistent issue. Clinical information held by the patient in the PHR cannot easily be sent to other providers electronically. Instead, patients must print their information and bring hard copies to their visits.

Connections between untethered PHRs and tethered PHRs are rare. This issue is partially resolved when a PHR vendor offers both a tethered and untethered PHR product, but even in that instance, the interface only impacts providers with whom the vendor has a relationship. This issue limits the number of providers with whom the patient can share data. The interface is expensive for providers. Providers pay interface costs as well as maintenance costs for every interface, and these expenses become a significant barrier for providers accessing and receiving data electronically from untethered PHRs.

This issue can be resolved by connecting tethered and untethered PHRs to a central hub such as an HIE, or through a standard messaging service such as Direct. This type of exchange is provided in the MU2 criteria, but the rules do not specifically state that an HIE is the preferred method of exchange. Health information exchange, whether through a state or regional-level service or through the use of Direct secure messaging, can provide a way to manage patient records, identity, and privacy and security and reduce the number of connections or interfaces required.

3.2.2 Pilot to Demonstrate Bidirectional Data Flow

The promise of using PHRs as instruments to improve patient-centered care has been recognized in the literature over the last few years.[3] A true patient-centered PHR would represent a complete patient health care record and allow data sharing across health care settings and systems. The environmental scan and discussions with stakeholders identified several valuable attributes of both tethered and untethered PHRs, but neither approach is designed to produce a complete patient health care record. We found that tethered PHRs (patient portals) are well-integrated with health care facilities' EHRs and that data flow

[3] Reti, S. R., Feldman, H. J., Ross, S. E., & Safran, D. (2010). Improving personal health records for patient-centered care. *Journal of the American Medical Informatics Association, 17*:192-195. Available at: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3000780/

between these two systems is seamless. However, integration between a tethered PHR and other systems (such as an untethered PHR or a tethered PHR in another health care enterprise) is fairly limited; hence, tethered PHRs usually do not include information associated with health care provided by other entities. Similarly, the functionalities of untethered PHRs vary, with some requiring patients to manually enter data to ensure a complete patient health care record and others providing for automated data integration from other systems.

Collaboration with the Regional Extension Center to Support PHR Pilot Project

Under the auspices of the Office of the National Coordinator for Health Information Technology's Regional Extension Center (REC) Program, a pilot was initiated to understand interoperability between various systems during creation of a complete health care record. The three objectives of the pilot study are to (1) explore opportunities to improve patient-centered care using bi-directional exchange, (2) identify "use cases" to demonstrate the value of exchanging patient-generated data with the provider and (3) develop user guides to support bi-directional exchange and help patients share data across tethered and untethered PHRs.

Some early findings from the pilot indicate that patients have to possess a certain level of technical skill to complete the various steps needed to create the enhanced patient record and send it to their provider. More information is available regarding the pilot in **Appendix A**. The implementation guides are provided in **Appendix B**.

3.2.3 Personal Health Records and Health Information Exchange

PHRs vary in their ability to interoperate with providers. Untethered PHRs are less likely to offer visit-related functionalities, such as appointment reminders or provider messaging. They do, however, allow for more data control by the user, such as identifying the providers who have access to or receive data.

Leveraging health information exchange, either referred to as a service or a general concept, could offer a superior PHR for the patient. Barriers to offering a PHR include the following:

- *Inability of the HIE to interface directly with the patient:* Functionality would need to be developed for the provider to authenticate the individual.
- *Liability:* The risk increases for the HIE as more entities/individuals are allowed access.
- *Disclosure:* Legal requirements related to certain types of treatment, such as family planning, may be an issue for HIEs (i.e., identifying disclosures that are appropriate and how an HIE would deal with documenting these disclosures).

Although these issues need to be addressed, HIEs offer some unique advantages, including the ability to do the following:

- Standardize inbound and outbound data.
- Provide a single interface for providers.
- Provide patients access to a more comprehensive record that includes data from many different providers and hospitals.
- Provide access to payor claim data.

3.3 Payor and Provider Adoption and Implementation

3.3.1 Language Options

Findings from the environmental scan and discussions with stakeholders show that effective implementation of a tethered PHR requires detailed planning. Health care facilities expressed a clear preference for PHR functionalities that improve adoption and use. Providers identified a clear need to support users who speak a primary language other than English. This requirement is important for stakeholders in New Mexico. miVIA, developed for migrant workers and offered in Spanish, is the only PHR included in the environmental scan available in a language other than English.

Developing PHRs in different languages may not be practical, since providers may want to operate in an English-based PHR. Instead, we recommend that PHR vendors support views of the PHR in different languages, allowing the user to choose the language. Implementing a PHR with a translator function that operates in real time is a challenge but will help improve use among diverse users. This requirement may perhaps be addressed in workgroups tasked with developing standards to improve interoperability between health information systems.

3.3.2 Workflow

Proper implementation is vital to ensuring utilization of any new technology and was a common theme throughout discussions with key stakeholders. Multiple participants mentioned that the longest, and often most difficult, phases of implementation included understanding their workflow and then identifying the individuals responsible for each area of the workflow. Although PHR systems differ in functionality, the discussions identified three key areas of consideration that are common across PHR workflow: (1) patient access, (2) data maintenance, and (3) customer support. Note that this section focuses only on findings from provider and payor discussions, and refers only to tethered (HIPAA-covered) PHRs.

Patient Access

The first implementation issues addressed are often protocols for granting and validating access. Regardless of PHR vendor, each participating provider organization developed a method to verify patient identity. Most participants indicated that individual patients and patient-authorized representatives were required to verify in person that they were the appropriate party to access the PHR information.

Once authorized users were verified, they were assigned temporary usernames and passwords either via e-mail or printed information sheets. This step introduced a variety of obstacles to enrollment. In one participant's practice, patients often lost the paper copy that was provided with their login information. For security purposes, the practice would not supply a replacement copy until the patient physically returned to the practice. For participants using digital communications for account creation, patients often ignored the e-mails or the emails went to the recipient e-mail's spam filter; the result was that accounts were never created. These issues involve the staff who are responsible for setting up accounts, providing information for login, and troubleshooting issues that arise. Account creation was typically assigned to front office staff so these staff members needed training address enrollment issues.

Data Maintenance

Another PHR workflow issue concerns the maintenance of patient health information in the PHR: how will sending this information to the PHR be incorporated into clinical workflows? Another consideration is the approach to populating the PHR with new clinical information. The provider was typically the person identified to populate the PHRs; however, multiple participants indicated that this process was often cumbersome and was not easily integrated into current clinical workflows.

A related workflow issue is the need to identify the information made available to patients. The information provided to patients via PHRs varied significantly. For example, providers had differing levels of comfort with providing lab result data to patients. In many cases, the providers did not want to provide lab results via PHRs to patients until after they had communicated them to patients in person or over the phone. Providers felt that unnecessary stress could result from patients accessing this information without explanation.

Customer Support

A last workflow consideration is determining how to support customer requests and needs. This area was identified multiple times during our discussions as a need that was overlooked or under-resourced during initial planning, but was an absolute requirement once the tethered PHR, also known as a patient portal, went live. In most cases, front office staff members were assigned to handle all questions and troubleshoot issues from patients trying to use the tethered PHR. In general, participants described this issue as a significant burden

for staff and an assignment that required training and familiarization with the PHR technology.

3.3.3 Business Case

Another key finding from discussions with providers, health care systems, and payor representatives is that there are business-related advantages associated with PHR implementation. The most common benefit identified was a higher rate of bill collection. The introduction of claims and billing features in their PHRs allows patients to view their claims status, view their payment history, and pay bills when applicable. According to some of the payors, the ease of this functionality actually led to another benefit: higher consumer satisfaction scores.

Multiple participants indicated that the implementation of PHR technology eliminated many of the calls previously handled by front office staff. This development helped justify the time and cost of retraining front office staff to support PHR functionality, which was time consuming and costly during start-up. Furthermore, in some cases, the ability for patients to input their own information into the PHR allowed additional time savings at check-in once the patient arrived at the office.

Another business case for PHR implementation was the desire for the provider organizations to reduce the burden associated with achieving the Centers for Medicare & Medicaid Services' EHR Incentive Program's Meaningful Use criteria. By achieving these criteria, the providers and hospitals would simultaneously become eligible for incentive payments and avoid the Medicare reimbursement penalties. These payments would help to offset any costs of the implementation of the PHR and EHR technology. Although most did not specify which criteria were being addressed through using their PHRs, multiple measures are supported by PHR functionality, including providing patient education, providing timely online access to health information, providing electronic copies of health information upon request, and providing clinical summaries.

3.4 Consumer Adoption

3.4.1 Technology and Language Barriers

Discussions with key consumer advocates and lay consumers yielded some findings that mirrored the concerns expressed by providers; namely, that Internet access and language barriers were important issues with no easy solutions. These issues are particularly salient for New Mexico, given that the state ranked among the highest in the nation regarding technological disparities between rural and urban communities and approximately one third of residents speak a primary language other than English.[4] As noted previously, only one of

[4] U.S. Department of Commerce, National Telecommunications & Information Administration. National Broadband Map. http://www.broadbandmap.gov/. Accessed March 07, 2014.

the PHRs we reviewed was available in another language. However, one consumer revealed that although English was her second language, she greatly valued the PHR because she could see and then look up any words her physician had used that she did not understand.

3.4.2 Limited Awareness

The next barrier we identified was limited awareness of untethered PHRs. In general, people were aware of tethered PHRs, or EHR-tethered patient portals, but none were aware of the non-HIPAA-covered, or untethered, PHRs. Particularly in Utah, most consumers receive health care from one of two large systems, each of which has a tethered PHR, and most consumers knew about these although actual use was mixed. Few consumers reported being encouraged by their provider to use these PHRs. Most saw posters or heard about it in other ways, suggesting that providers could greatly increase use by discussing their PHR with patients. In this case, front office staff could be leveraged to assist with sign-ups and technical problems, although budgeting and planning for this change in the workflow would require some planning, as noted above. Consumers suggested that community navigators, for example in senior centers, could assist with PHR use as well.

3.4.3 Health and Technology Literacy

Because patients with low health literacy tend to have worse health, this population could benefit from the use of PHRs to manage their health.[5] Even savvy consumers can experience a significant burden in using currently available applications as a single comprehensive record. Staff working within the health care community could be used to help those with low health or technology literacy become more comfortable with online tools to help them manage their own health care. These navigators provide an important role in ensuring PHRs support the users' needs. Tethered PHRs require setup and password retention, and untethered PHRs require time and technological ability to integrate multiple data sources or to enter information manually. We recently demonstrated this challenge in the REC pilot described above. Again, providers and navigators can assist with this issue; however, the time costs may be high.

3.4.4 Distrust

Another barrier that providers and PHR advocates will have to contend with is public distrust. Many, but not all, consumers trusted their providers and felt that the information in a tethered PHR was sufficiently secure. Utah consumers especially expressed mistrust of government, health care reform, and the commercial interests behind untethered PHRs. Consumer adoption of these types of PHRs could improve with stricter data use requirements, such as providing similar protections as the HIPAA Privacy Rule to those systems not currently covered as business associates to a covered entity. Consumers

[5] Baker, D. W., Wolf, M. S., Feinglass, J., Gazmararian, J. A., Thompson, J. A., & Huang, J. (2007). Health literacy and mortality among elderly persons. *Archives of Internal Medicine, 167*:1503–1509.

generally saw the value in being able to aggregate all of their health data in one place, which is possible with an untethered PHR, but for most, the benefits did not outweigh the concerns.

3.5 Data Control

3.5.1 Control of Data and Data Quality

Historically, medical records have been perceived by providers as belonging to the provider. The paper record resided physically in an office, and though legally accessible to patients upon request, in practice this could prove cumbersome for the patient. The introduction of PHRs created a new, potentially easier way for patients to access their medical data and for providers to release those data. Many PHRs, especially tethered PHRs, provide consumers view-only access to parts of their medical record. In this case, consumers who notice errors can request fixes directly through their provider, which many consumers view as an advantage of PHRs—improving the accuracy of medical records. Some tethered PHRs allow consumers to edit what is usually consumer-supplied content such as smoking habits or family history. At least one PHR examined asked providers to accept or reject consumer-entered changes after they were made. This analysis assessed only a subset of the field types that could be changed by consumers, along with the mechanisms for reintegrating the information into the EHR.

Untethered PHRs offer much more data control to consumers. Consumers can decide what data are added and in many cases, can selectively import, delete, and modify information even when it is integrated automatically, such as from a continuity of care document or self-tracking device. The REC pilot demonstrates that even blood sugar readings uploaded from a glucometer could be manually changed in the test PHR. Some consumers find this level of control of their record ideal; these consumers have the most sense of ownership of their record and often want to control who can view it, and choose which parts are shared. This level of consumer control creates a new and important tension: a fully modifiable record allows for true patient-centeredness and empowerment, yet raises physician concerns about record completeness, accuracy, and patient safety.

Providers rely on accurate and reliable information to deliver appropriate patient care. Conversations with providers revealed that many were interested in having access to new kinds of data, such as blood pressure tracking device records, but said they could not trust information a consumer could modify. Establishing provenance of data will be an important enhancement if providers are to fully embrace data from patient-controlled PHRs.

[This page intentionally left blank.]

4. RECOMMENDATIONS

4.1 Privacy and Security

- Clarification is needed on the privacy and security provisions of PHRs. A common criterion, similar to the HIPAA Notice of Privacy Practices, is needed so that PHRs may be independently rated. Related to this, simplified user agreements that explicitly state, in plain language, how and when a vendor may use consumer protected health information are also needed. Both of these provisions may promote consumer awareness of and trust in PHRs.

4.2 Standards

- In order for PHRs to seamlessly integrate with other data sources, vendors need to work toward standardized messaging and exchanges. HIEs play an integral role in exchanging data and managing records from disparate systems and providers of care. Leveraging this infrastructure to bring data into patient records from untethered PHRs and payor PHRs will allow the patient to share data across a variety of care settings.

- We recommend that tethered PHRs develop interface connections with standalone PHRs, such as Microsoft HealthVault and its equivalents, to allow for automated data population. The support of this functionality will not only require technical collaboration between the health care facility (and the patient portal vendor) and the standalone PHR vendor, but will also require relevant data use agreements and BAAs.

4.3 Encouraging Consumer Awareness and Adoption of PHRs

- Increasing consumer awareness of all types of PHRs is a key first step to adoption. Most consumers were aware of tethered PHRs, though not all had used them; none that we spoke with were aware of untethered PHRs. Health care providers and consumer advocates can increase awareness, but in many cases, awareness alone will not suffice to achieve adoption. They will also need to help consumers sign up and provide ongoing technology support. Specific subpopulations would most benefit from PHR use: those with rare diseases (Crohn's), chronic conditions that require self-management (diabetes, asthma), or diseases that involve multiple providers (cancer, elderly people with comorbidities). Because PHR utilization at this stage in technological development is not always straightforward, especially for those who are unwell or otherwise disadvantaged, tech-savvy caregivers and parents of children with serious health problems may be effective early adopters and could be a focus of future, targeted adoption efforts.

- Consumer adoption of PHRs can be influenced by providers and front office staff, who are in a position to help consumers sign up and encourage ongoing use. Workflow adjustments will be needed to allow for routine support of PHR users. Providers can also encourage use by selecting a user-friendly PHR and setting up a number of features that have clear utility for consumers such as secure messaging, appointment scheduling, and viewing laboratory results. Providers must also reassure consumers about the security of their data, after taking steps to determine that data are indeed both technologically secure and protected by HIPAA.

- Community navigators can be leveraged to support consumers using a PHR, decreasing the burden on providers. Given the current usability of most PHRs, only

the most tech-savvy consumers will be able to go beyond basic PHR functionalities, particularly in the case of untethered PHRs, which require extensive manual typing or complex integration of multiple data sources. Live support will be essential for most consumers.

- PHR advocates at the government level should be cautious of consumer perceptions about government intrusion into health care. A key role for government, however, can be pursuing greater consumer protections for health data in non-HIPAA-covered PHRs. One suggestion is to design a rating system that would not constrain the private PHR market but would alert consumers to a given company's data use policies and level of technological security without requiring them to wade through complex documentation. From a government standpoint, preempting the negative consequences of a data breach by addressing data use policies and security concerns will be important to encouraging PHR adoption in the future.

4.4 Bidirectional Data: Define the Value for Patients and Providers

- Based on the discussions we conducted with patients and providers, we found a huge gap in awareness of the utility of sharing information between the two groups. Data ownership, security, privacy, and integration with workflow are some issues that need to be addressed to obtain consumer and provider support. Providers are wary of integrating information edited by patients into EHRs and using this information for clinical decision making. Patients, on the other hand, had varied opinions on the need to update their health care information. Some patients indicated that they would like to view the information present in their health care record, and they approved of systems that allowed them to correct any errors. Other patients mentioned that they trust the provider to maintain their health care information and were not interested in viewing their information.

- These insights indicate the need for research that explores the value of bidirectional information exchange from both provider and patient perspectives. Establishing rules and guidelines regarding the provenance of patient-generated or patient-entered data will be important to address provider concerns about data accuracy and liability issues.

4.5 Best Practice for Implementation

- We found that implementing PHRs and getting buy-in from providers and patients requires a multifaceted approach. The health care facilities that were successful in getting providers and patients to use tethered PHRs made significant workflow changes, trained office staff, supported features that patients and providers found useful, advertised widely, and actively enrolled patients. However, improving adoption of untethered PHRs requires a different approach. Untethered PHRs that are not connected to tethered PHRs have limited utility because the onus of maintaining the information is on the patient. However, enabling information flow between untethered and tethered PHRs would result in a more convenient and complete patient health care record. Currently, there are no standards for untethered PHRs to facilitate interoperability between these records, tethered PHRs, and eventually EHRs.

- Considerable work is being performed to facilitate data exchange between tethered PHRs and EHRs, and it would be advantageous to explore these standards in the context of untethered PHRs.

4.6 Cost and Incentives

- The CMS EHR Incentive Program must continue to be a focus for providers implementing PHR technologies as many of the requirements, and therefore the payments or penalties, are directly tied to the use of PHRs. Since 2011, eligible providers and hospitals have been striving to achieve the Meaningful Use criteria. Although these requirements focus on multiple aspects of incorporating clinical workflow/data into EHR systems, some of the measures can be specifically addressed using PHR technology. **Appendix C** outlines the Stage 1 Meaningful Use requirements that may be met by PHR technology. All of the listed Stage 1 Meaningful Use core requirements, and most of the menu set requirements, can still be achieved without the use of a PHR; however, in 2014 an additional Stage 1 measure will require providers and hospitals to make more than half of their patients' health information available online to view, download, or transmit to another setting of care. In addition, Stage 2 begins in 2014 and will include additional requirements that can be achieved using PHRs, and it will be unlikely that providers will be able to pass requirements without the use of PHR technology.

- The CMS EHR Incentive Program and the Medicare reimbursement penalties directly affect the overall cost associated with EHR and PHR technology. The incentives for eligible providers can net up to $39,000 over the remaining 4 years of the program if providers are Medicare eligible (with 2014 as the final starting year) or up to $63,750 for Medicaid-eligible providers over a 6-year period (with a final starting year of 2016).

- Hospital incentives vary significantly based on each hospital's specific discharge-related information, but they can receive millions of dollars depending on their incentive calculation. Although these totals may not cover the entire cost of the EHR and PHR technologies implemented at each organization, they will certainly help to offset some of the associated expenses.

- If providers do not become meaningful users in the incentive program, they will be assessed penalties in their Medicare reimbursement. These penalties will take the form of a 1% loss in Medicare reimbursement in 2015 that will increase each year up to a 5% total if the provider or hospital continues to fail to achieve Meaningful Use. Although these penalties will begin in 2015, they began to be assessed on the Meaningful Use status of providers in 2013. These penalties will certainly contribute to cash flow concerns.

- Relevant to this project, these incentives and penalties are time limited, and providers may not continue to use PHR technology beyond the EHR Incentive Program if they have not experienced clear value from the technology. In addition, if late adopters of this technology see that their colleagues are not experiencing added value from the use of these systems, they will likely forego adopting PHR technology themselves. To sustain PHR adoption, we recommend the following:

  – Further research should examine the features and functionalities that provide the greatest benefit to providers, according to their specific scope of practice. For example, multiple participating practices identified the ability to provide education materials to patients as one of the greatest benefits of PHR implementation. Leveraging informal opportunities, such as association meetings, local community initiative meetings and conferences, would also be useful to assess value of these education materials. Providers could network with colleagues and their professional organizations to identify which PHR

functionalities have provided the greatest benefit, so that they can make educated decisions on which functionalities to incorporate into their workflows.

– To promote PHR adoption, more attention should be devoted to start-up and maintenance costs. Providers need help understanding and budgeting for these costs. For many participants, training support personnel was a significant concern. Maintenance of the technology included the initial setup of accounts, support for lost passwords and access information, triage of secure messaging with providers, problems with scheduling appointments via the PHR, and general troubleshooting. Insufficient and inappropriately trained support staff would undoubtedly lead to lower system utilization and lower customer satisfaction with the system as a whole.

  For any provider organization, time is money, and the inability to charge for time spent communicating with patients via PHRs' secure messaging systems was also mentioned as a barrier. Although the use of secure messaging has not been proven as a significant source of unbillable time for providers, the perception does exist, which poses a challenge to adoption. More research and education in this area is needed to determine whether billing for time spent interacting with a patient through the PHR is needed or would help support the use of secure messaging functionality.

APPENDIX A
Summary of Findings from PHR Pilot with HealthVault Facilitated by HealthInsight

The pilot focused on one independent clinic and examined existing mechanisms that patients can use to transmit data between the tethered PHR (Kryptiq) and an untethered PHR (Microsoft HealthVault). To explore the value of exchanging patient-generated data with the provider, we integrated data from devices, such as glucometers, with Microsoft HealthVault and transmitted this enhanced patient health care record to the provider using the 'Direct' communication protocol.

The user implementation guide that was developed will help patients and caregivers: (1) create accounts in Kryptiq and Microsoft HealthVault; (2) download a Continuity of Care Document (CCD) from Kryptiq and upload the data into a Microsoft HealthVault account; (3) connect and upload data from a glucometer to a Microsoft HealthVault account using the Connection Center Application that is available from HealthVault; and (4) download a CCD from HealthVault that includes data from the glucometer and then transmit the CCD to their provider via Direct.

The draft user implementation guide is provided in Appendix B and was developed using test accounts provided by the clinic. We conducted in-house testing of the guide with four users and a summary of the findings and challenges identified is presented below. Testing of the guide with patients at the clinics and the integration of the enhanced patient record with the EHR via an interface engine is out of the current scope of this pilot, but will be pursued in future initiatives. The current draft of the guide will be updated based upon the feedback received from testing at the clinic and other stakeholders. A final version will be made publicly available at http://healthinsight.org/about-us/publications. **Figure A-1** describes the flow of data across these various systems and illustrates the current scope of the pilot.

There are several challenges that need to be addressed before the promise of an enhanced patient health care record can be attained. Some of the challenges we identified are discussed below:

a) Patients have to possess certain technical skills to complete the steps necessary to create the enhanced patient health care record and send it to their provider. Despite the fact that patients do not have to write code to upload and parse data from the CCD to their HealthVault account, they may find it challenging to download the CCD from their patient portal, unzip the files, and identify the right file (XML format) to upload to their HealthVault account. We recommend that tethered PHRs develop interface connections with Microsoft HealthVault to allow automated population of data from the portal. As discussed previously, the support of this functionality does not only require technical collaboration between the health care facility (and the patient portal vendor) and HealthVault, but also requires relevant data use agreements and business associate agreements.

b) Most glucometers do not allow data to be uploaded to a PHR. Typical and current workflow involves patients bringing their glucometer to a clinic visit where the Medical Assistant manually enters the data from the glucometer. During the initial phase of the pilot, we tested four glucometers and were ultimately able to upload data, after several attempts, from two glucometers into HealthVault using the Connection Center Application. However, one of the glucometers required patients to manually enter the port number and most patients find it challenging to perform that task.

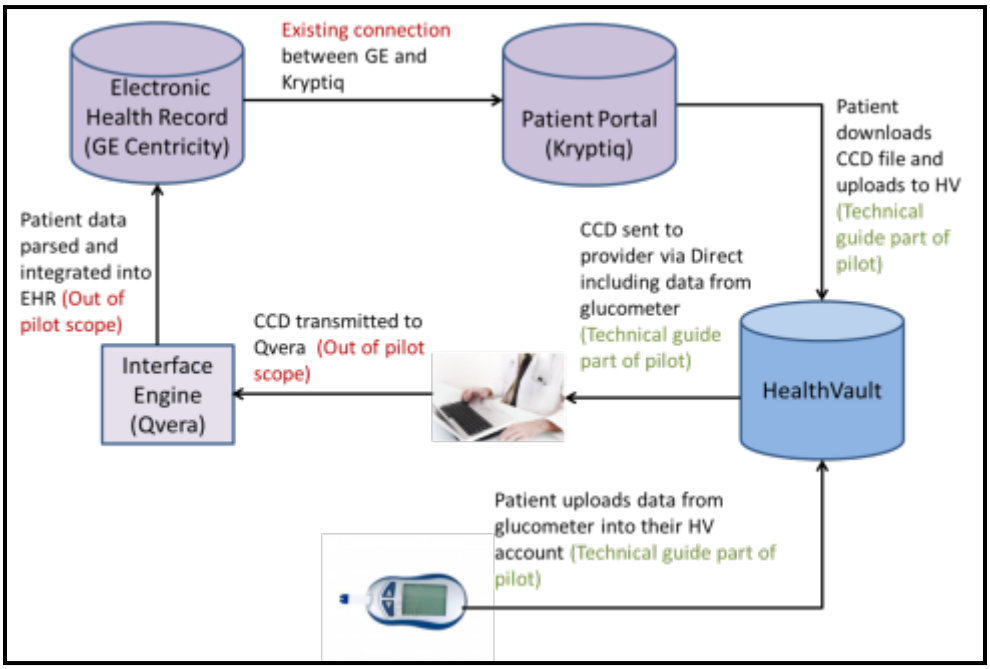
c) The user interface of Microsoft HealthVault makes it challenging for the user to identify the navigation pathway necessary to conduct some of the functions required in this pilot. For example, if users want to automatically populate their HealthVault account, they need to click on "I want to", which provides a drop-down menu, and from the menu, click on "Add or update health information". This displays another drop-down menu under "More Actions", from which the user has to click on "Upload a File" to get to the point where they can actually browse and upload the CCD.

d) We also found that patients can edit their data once they have populated their account. While the availability of this functionality is critical to the concept of patient-owned data, it poses a challenge in demonstrating the value of patient-generated data in clinical decision-making. Allowing patients to edit the data may make providers wary of this data. This may be resolved if the data sent to the provider is tagged indicating that it has been modified. However, the CCD that HealthVault currently creates does not include any such tags.

e) The other challenge was that Microsoft frequently updates HealthVault's user interface and the navigation pathways. During the course of this four month pilot we had to modify the user guide three times to ensure that it was up to date. These frequent updates pose a barrier to training patients and developing materials that remain up-to-date in the long-run.

The lessons and findings of this pilot are instrumental in ensuring that stakeholders understand the limitations of current mechanisms for data sharing and recognize the requirements needed to support bi-directional exchange.

Figure A-1. Dataflow Through the Systems Involved in the Pilot



[This page intentionally left blank.]

APPENDIX B
USER IMPLEMENTATION GUIDE

User's Guide to Share Data with Your Provider

January 13th, 2014

[This page intentionally left blank.]

Table of Contents

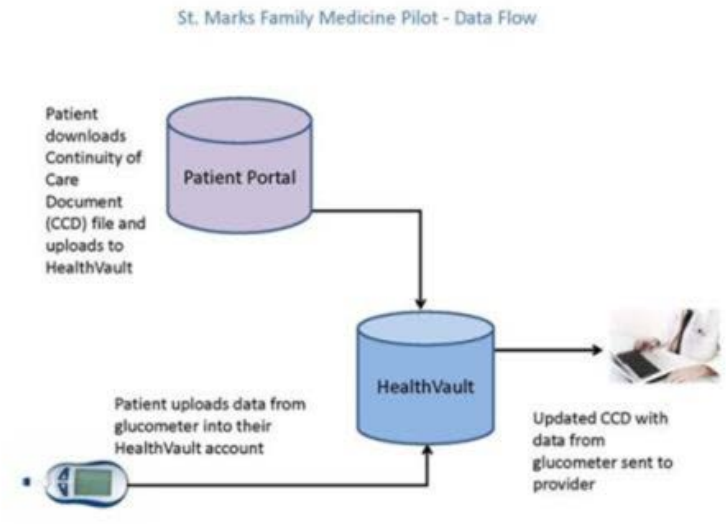
[This page intentionally left blank.]

Introduction

This patient guide is designed to help you store all of your health information in one place. A personal health record (PHR) can help you manage your health care needs. For example, you could look at your record to see what the result of your last cholesterol test was, and easily compare it to previous tests to see your progress. A PHR lets you add information from multiple doctors. You can also add information you gather yourself, such as family medical history or the readings from a blood pressure tracking device. Once you have all this information together, you can share it easily with doctors, family members or caregivers. A PHR can be in paper form, but we will be working with a web-based PHR.

There are many different kinds of PHRs and lots of different ways that you can get information from your doctor to your PHR. For this patient guide we will be showing one specific example. We will be using the "patient portal" of St. Mark's Family Medicine in Salt Lake City, Utah. A patient portal is similar to a PHR, except that it is linked to one doctor or health system. With a patient portal, you can log in to the website provided by the doctor and see certain parts of your own medical record. In order to get all of your medical information in one place, we will use a separate PHR, called Microsoft HealthVault.

This guide will show you how to get medical information out of St. Mark's Family Medicine's patient portal and into Microsoft HealthVault. Then we will add information from a medical device that is used for diabetes management, called a glucometer. A glucometer is used to test blood sugar levels by drawing a small amount of blood from the finger. Finally, we will show you how to send all this information back to your doctor, so he or she can have all your medical information in one place as well.



Before You Get Started

You will need:

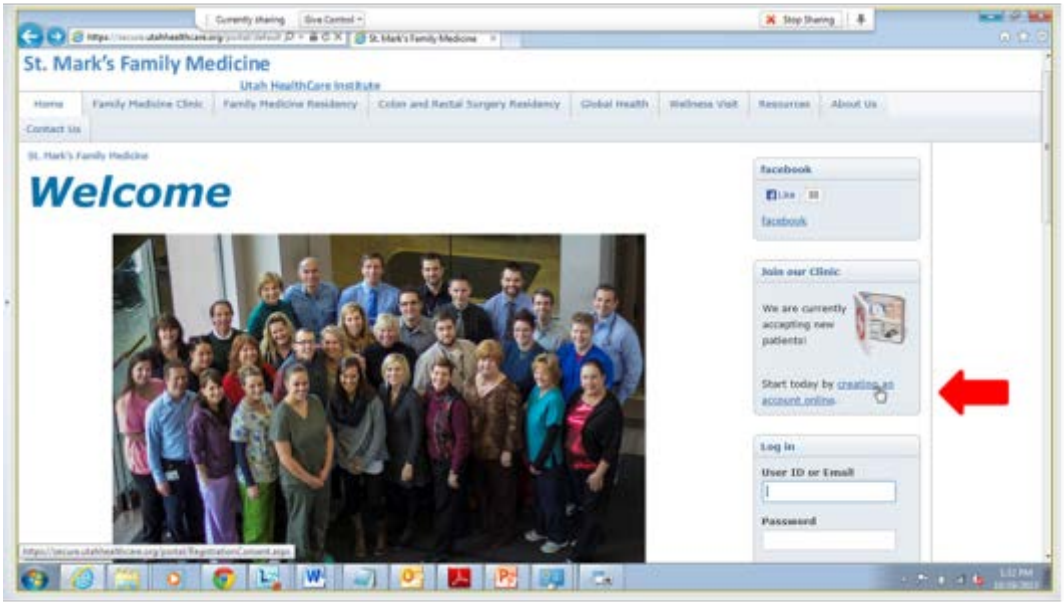
- a computer that runs Windows (a PC)
- a compatible glucometer (we recommend OneTouch Ultra2)

- a USB cord, to attach the glucometer to the computer

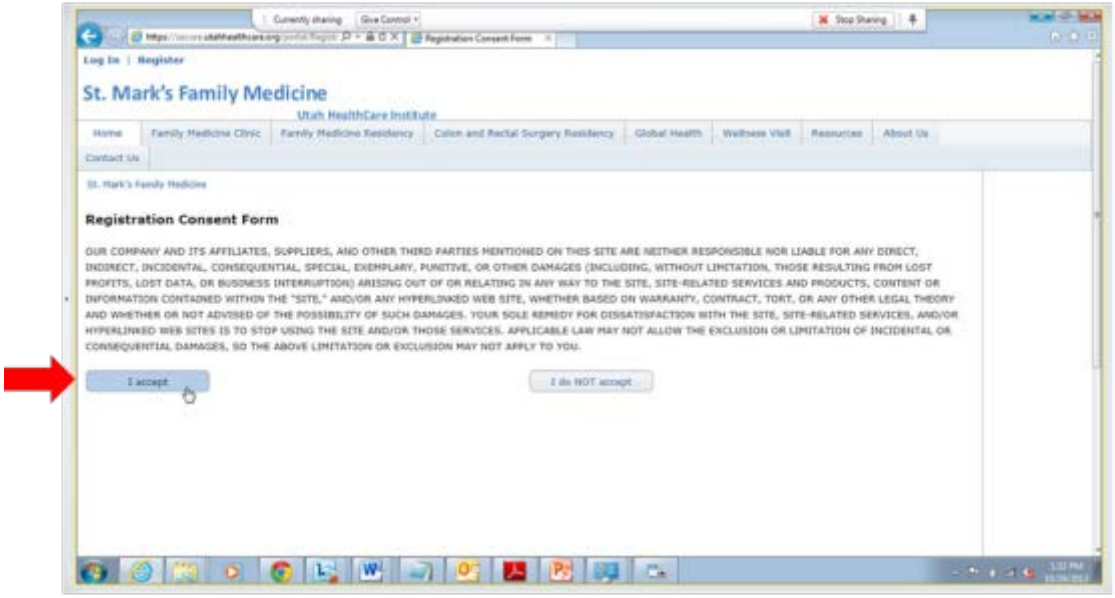
Create an Account in Your Doctor's Patient Portal

First we will create an account on your patient portal. You'll only have to do this once.

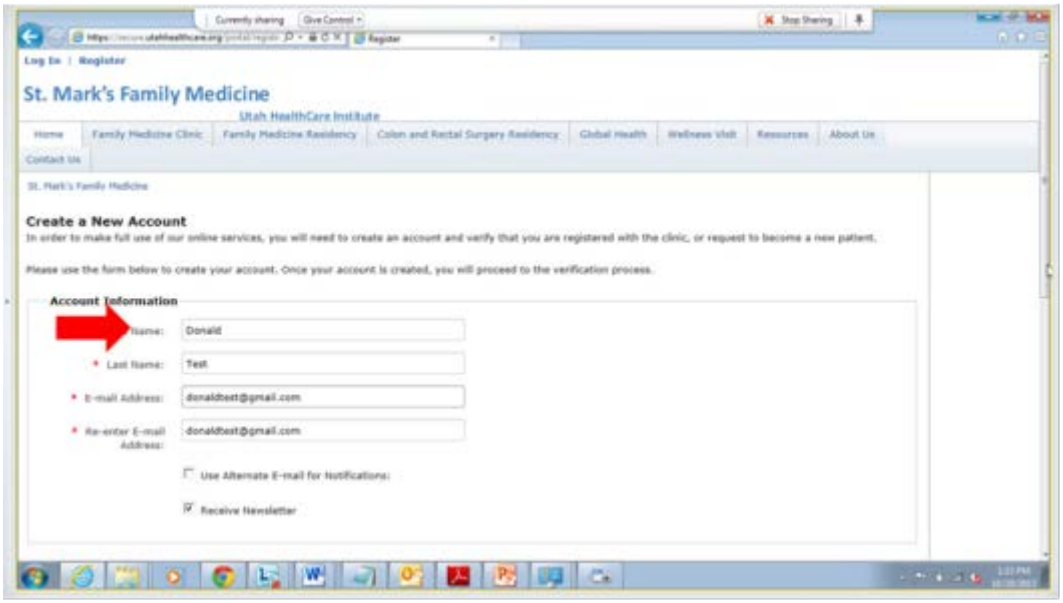
1) Turn on your computer and open up Internet Explorer (a web browser). It's very important to use Internet Explorer!
2) Go to your patient portal website: http://utahhealthcare.org
3) Click on **creating an account online**.



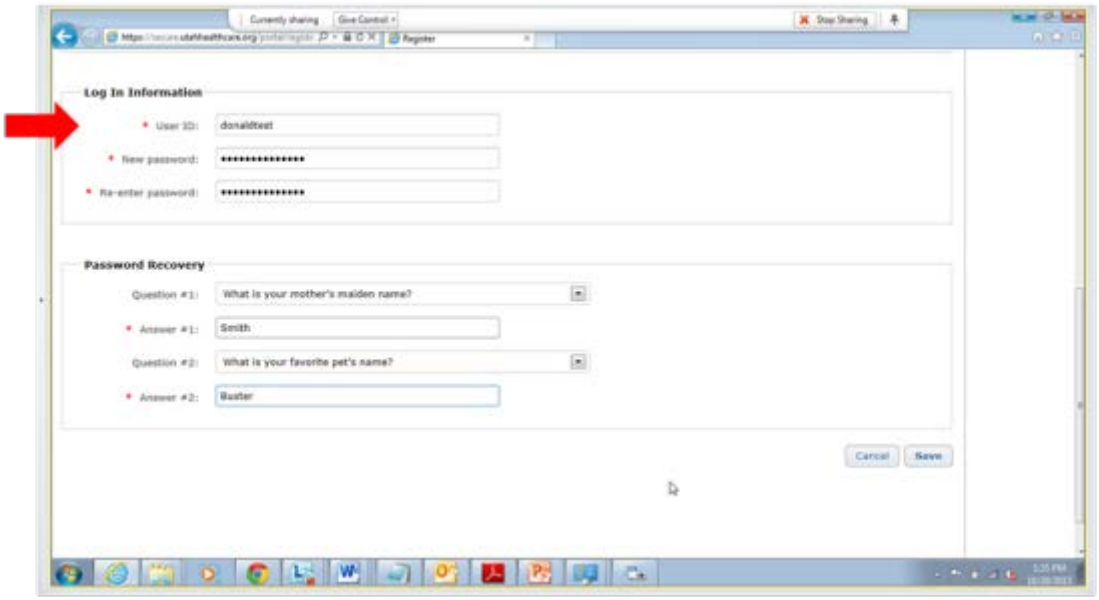
4) Read the consent form and click **I accept**.



5) Enter your name and email address.

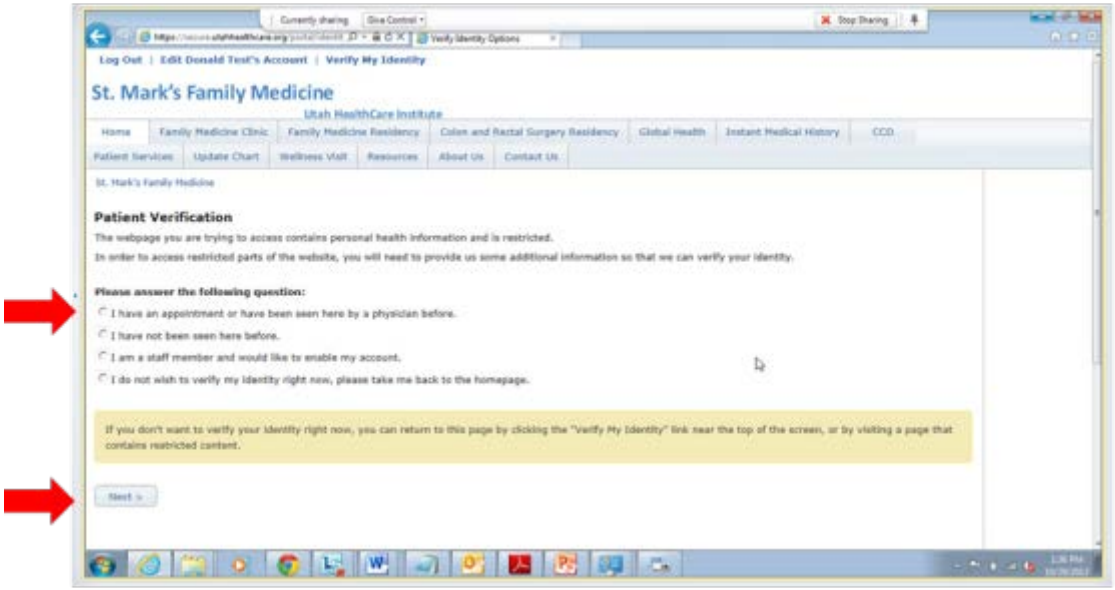


6) Create a user ID. It's a good idea to use your email address.

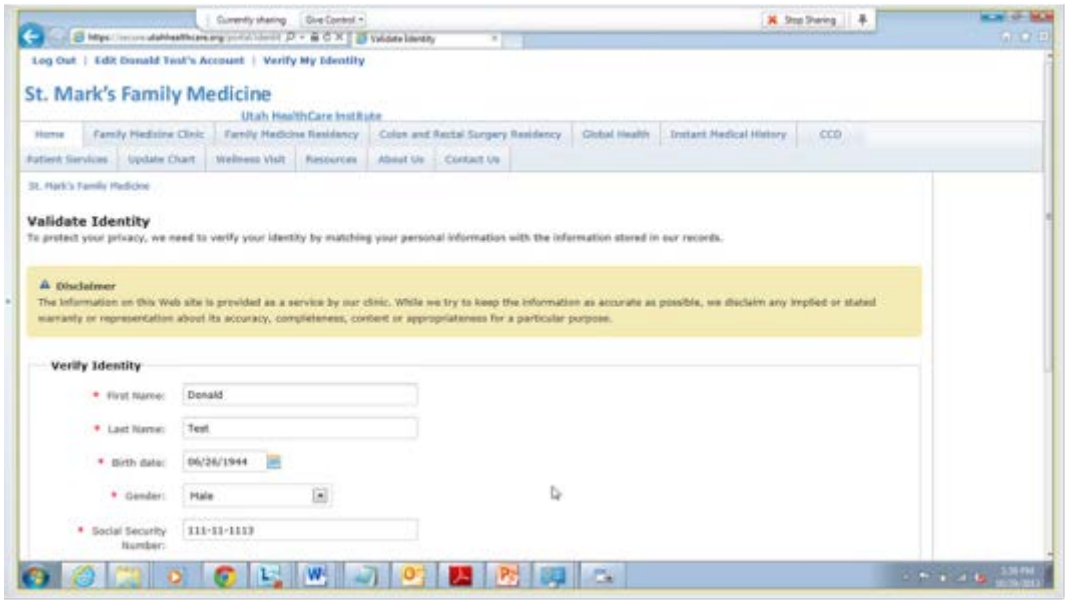


7) Choose a password and two security questions and answers.

8) Complete the Patient Verification page by choosing the first option. Click **Next**.

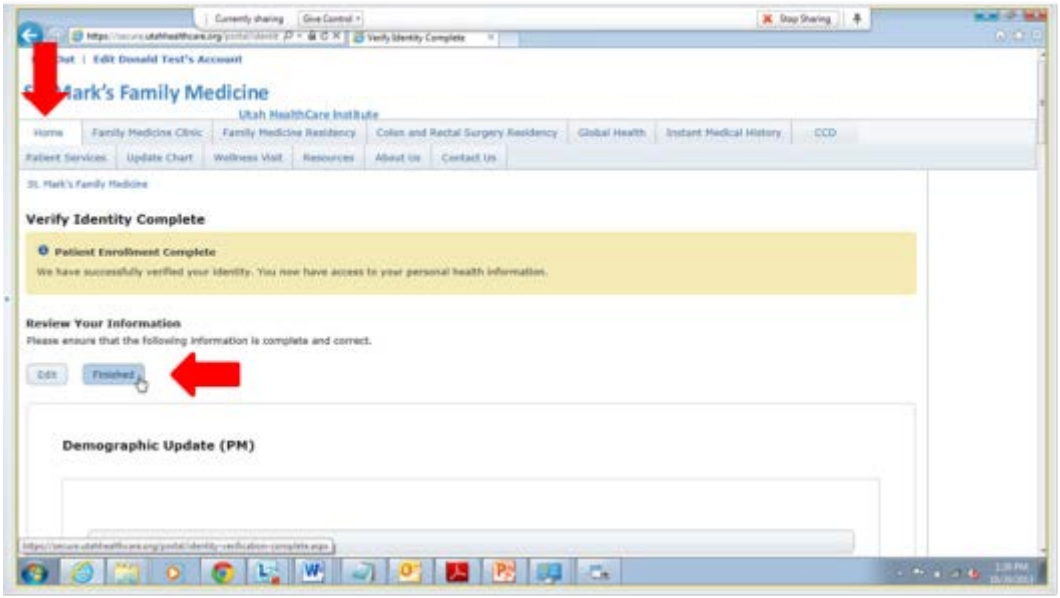


9) Follow the steps to validate your identity.



10) Click **Verify**.

11) Click **Finished**.



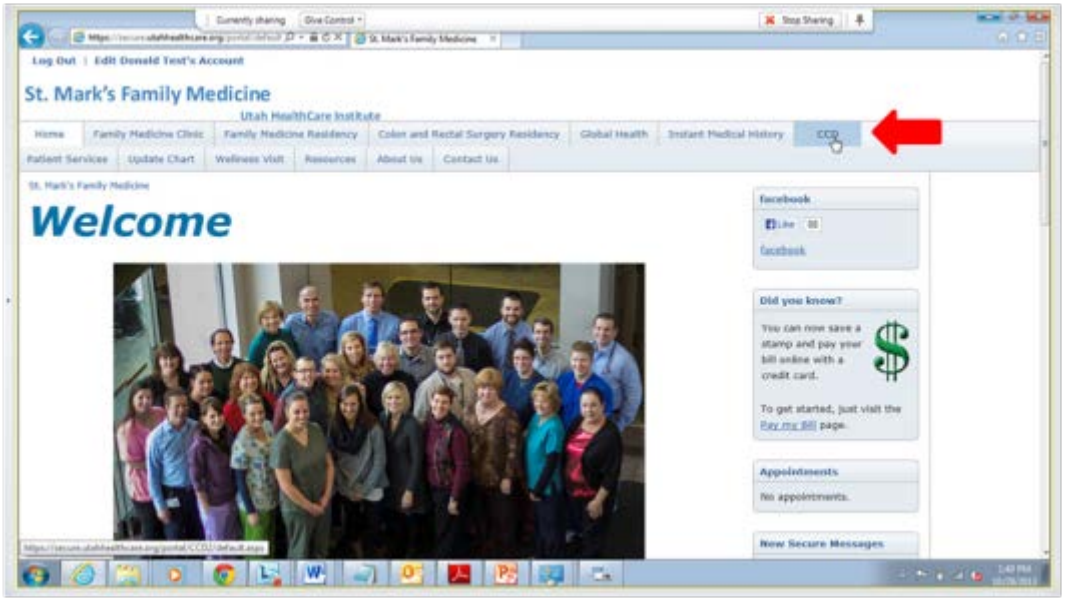
Click on the **Home** tab to return to the homepage.

Get Your Medical Information Out of the Patient Portal

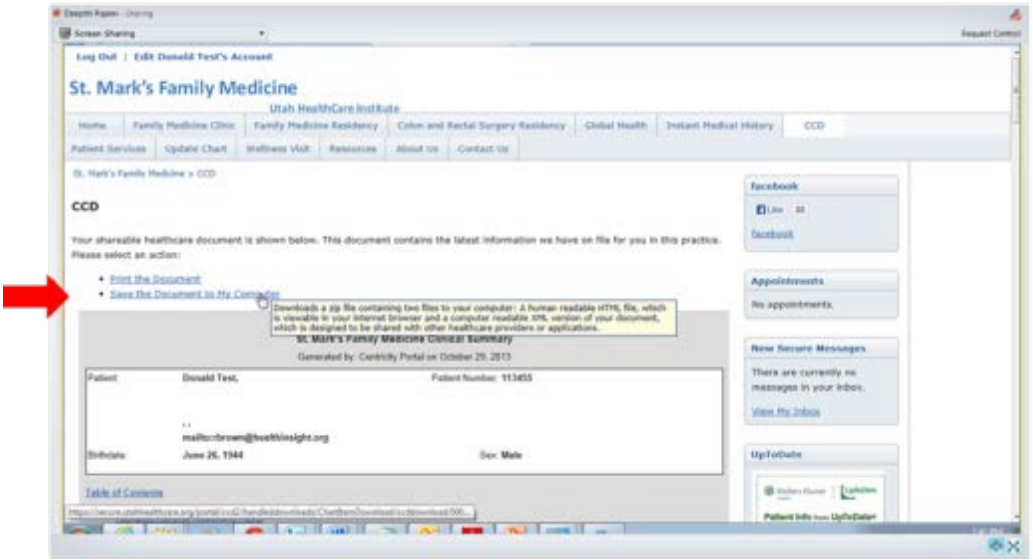
In this step you are going to export a file of your medical information from your patient portal, called a Continuity of Care Document (CCD). Then you will save it to your personal computer. You will do this step any time you want to get new information from your doctor's record into your PHR, such as after an office visit.

1) Go to your patient portal website: http://utahhealthcare.org. Log in with the user name and password you created in the first section.

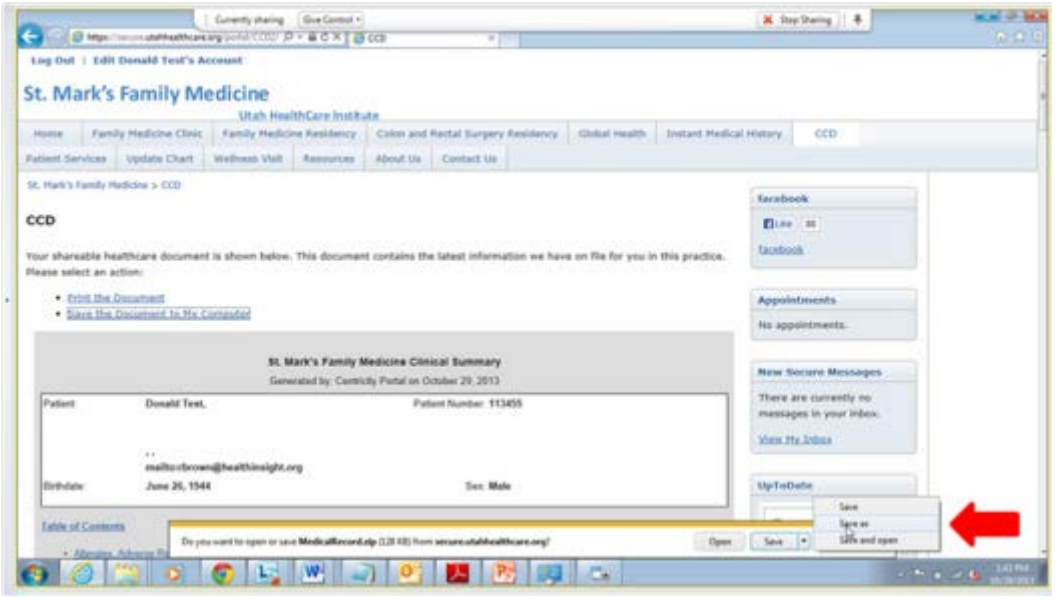
2) Click on the **CCD** tab.



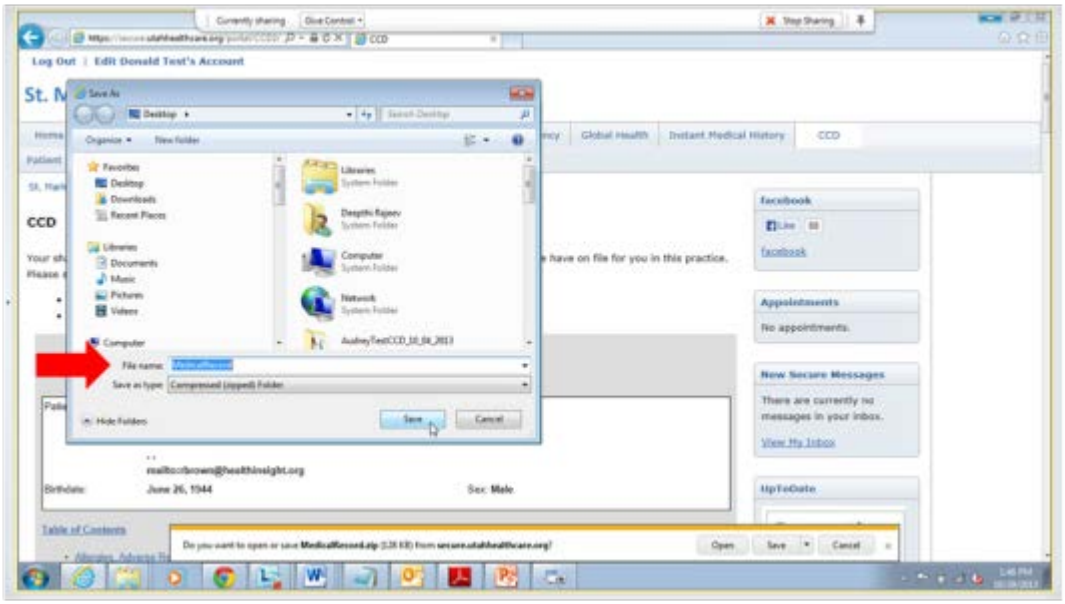
3) Click **Save the Document to My Computer**.



4) In the pop-up Download bar, click the small drop-down arrow next to the Save button and click **Save As**.



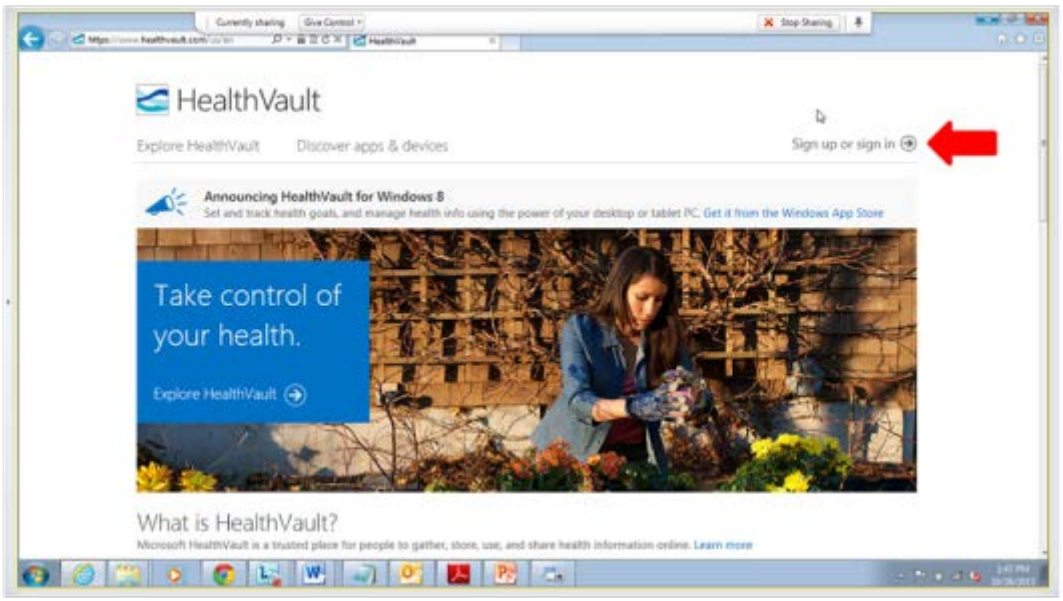
5) Choose a place to save the file. It's a good idea to save it on the Desktop with a file name that includes your name and the date. For example, CCD_Donald_Oct2013.



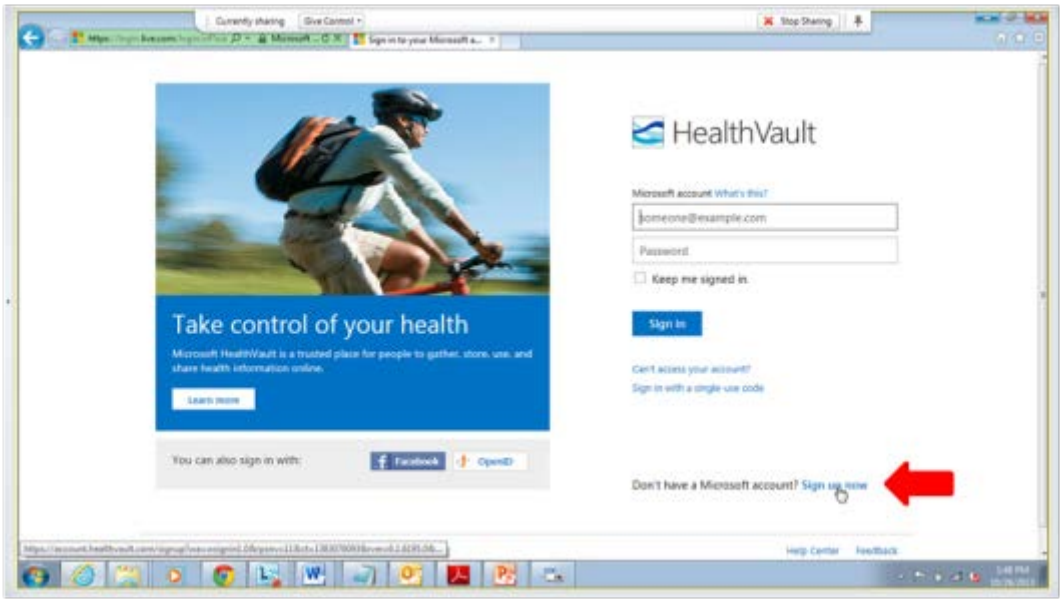
Create a Microsoft HealthVault Account

You'll only have to do this once. It's a good idea to keep your usernames and passwords in a **secure** place in case you forget.

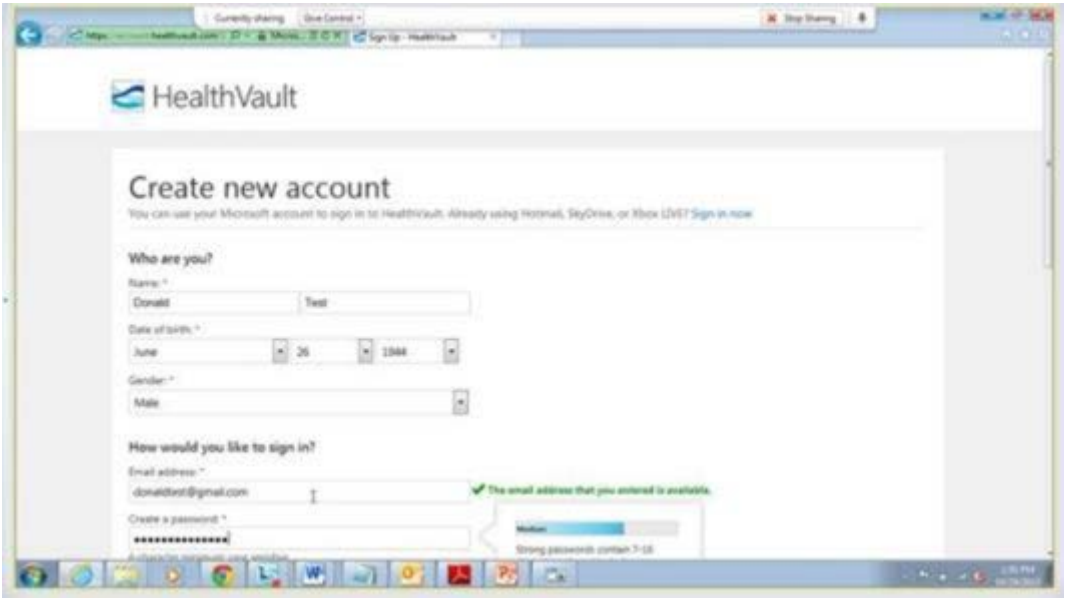
1) Using Internet Explorer, go to healthvault.com and click **Sign Up or Sign In**.



2) Click **Sign up now**.

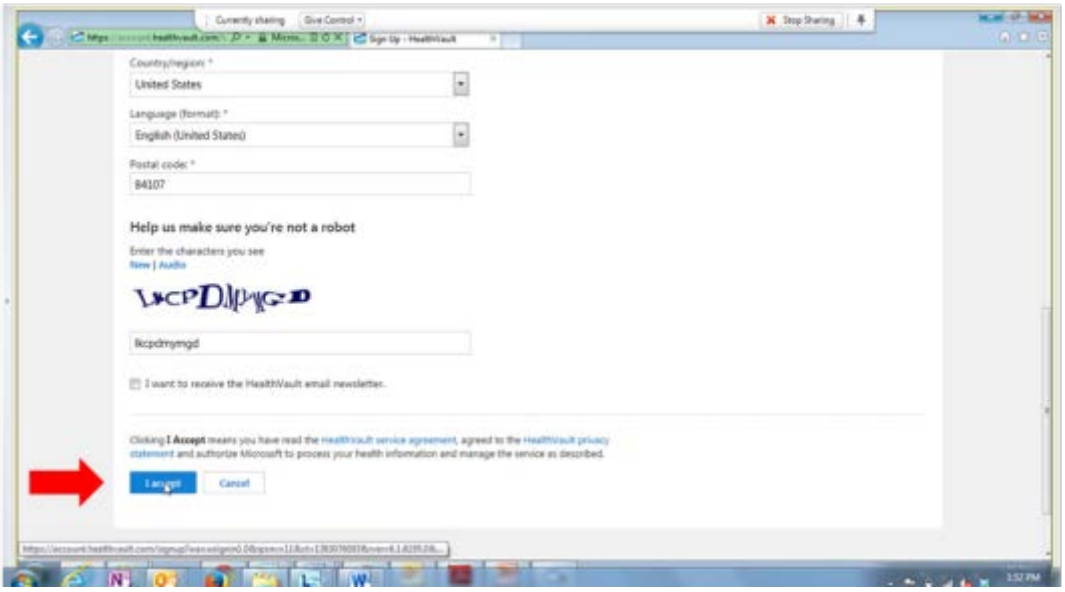


3) Fill in your information.

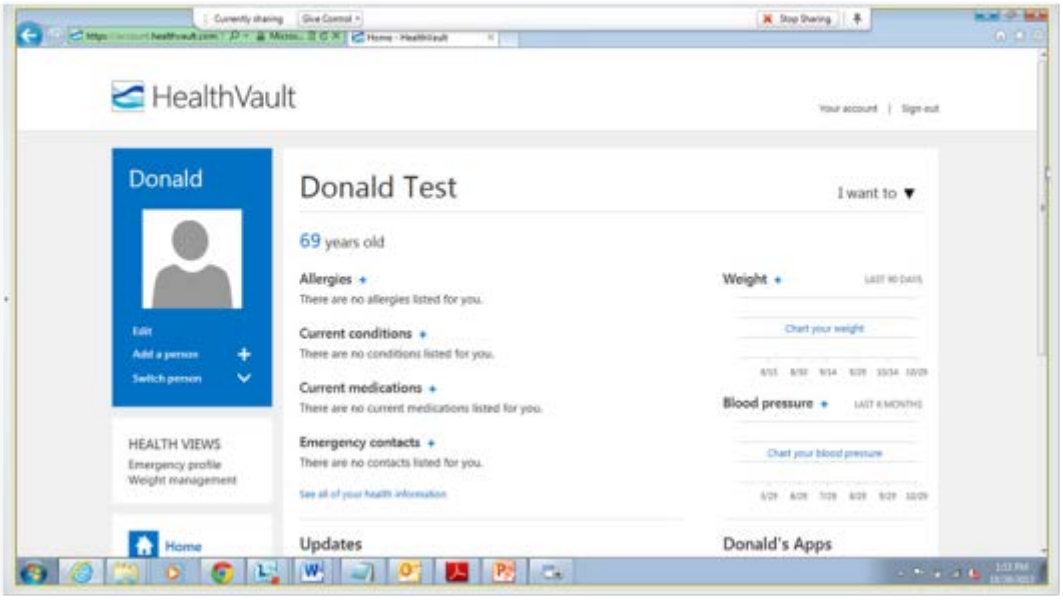


4) Create a password using the guidelines provided on the webpage.

5) Click **I accept**.



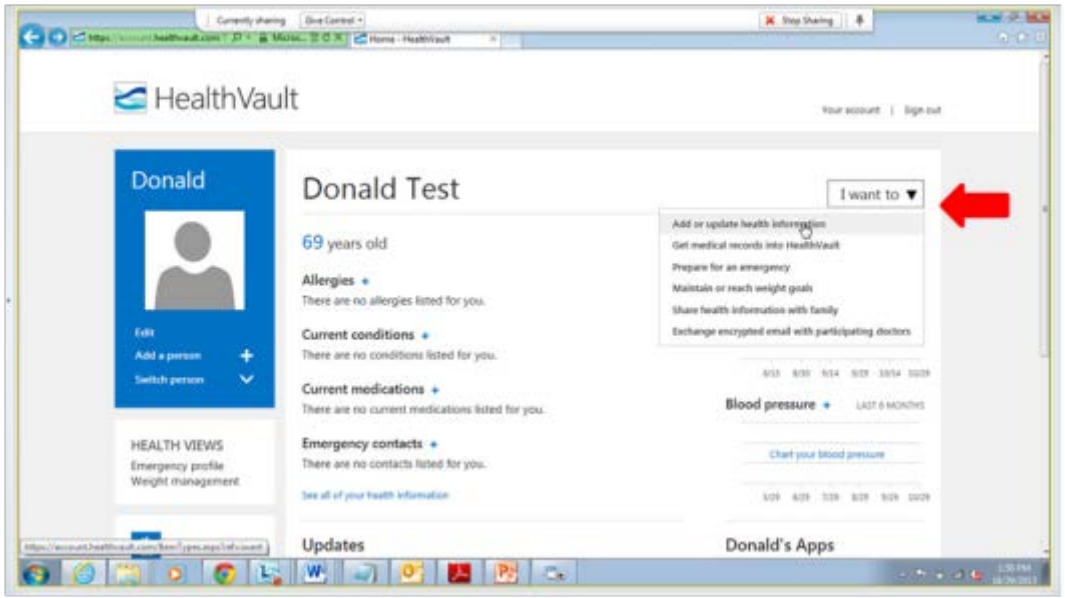
6) Your webpage should now display your HealthVault profile page and show a summary of the information you just entered.



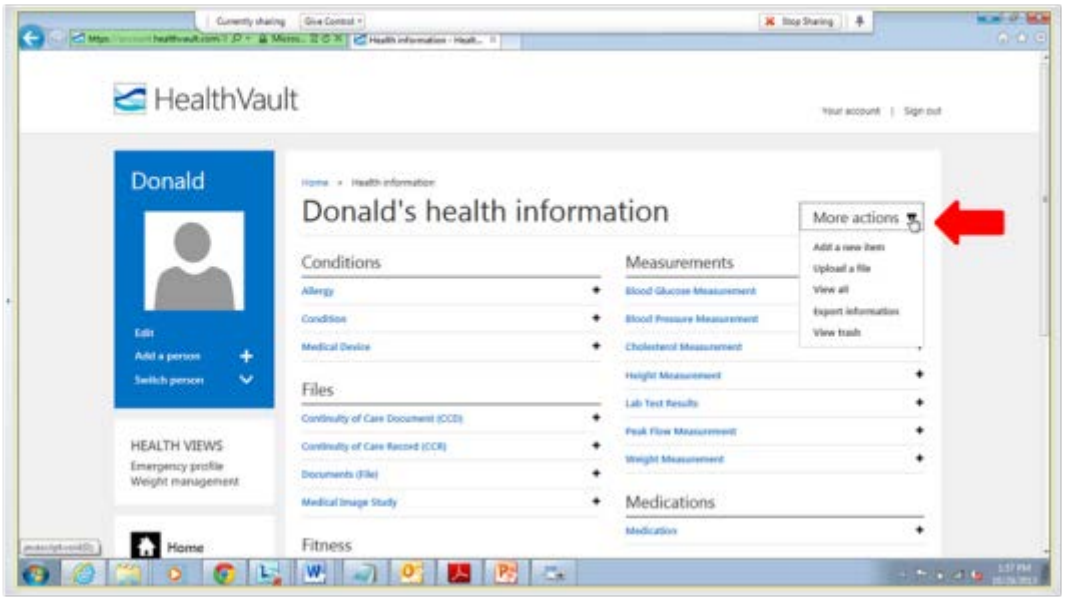
Get Your Medical Information into Microsoft HealthVault

Next you will use the CCD previously saved to your Desktop and send it to your HealthVault account.

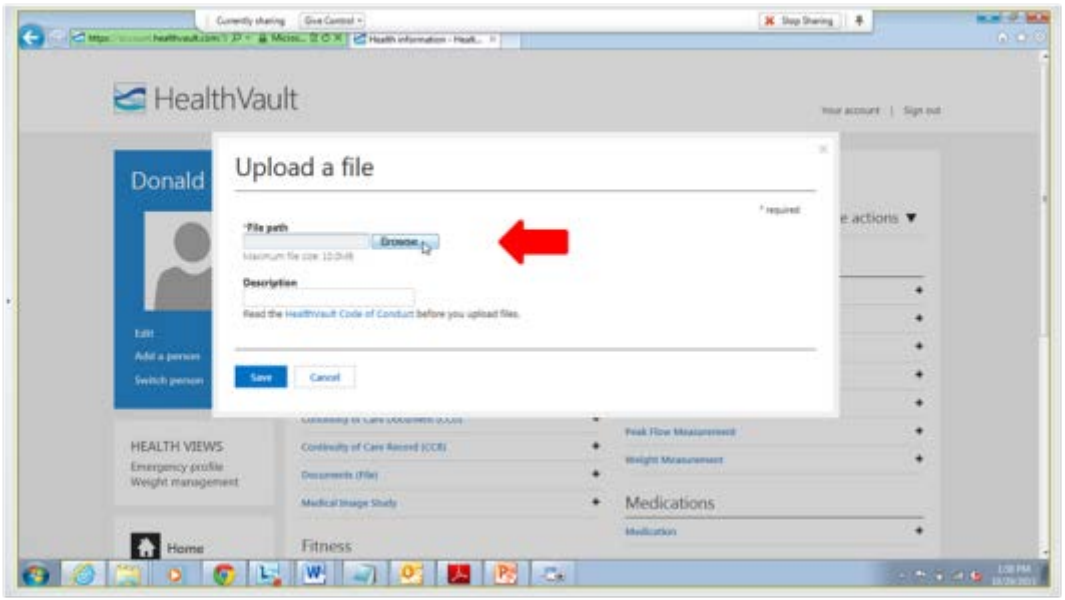
1) Log in to healthvault.com with the username and password you created.
2) Click **I want to** and then choose **Add or update health information** from the drop-down list.



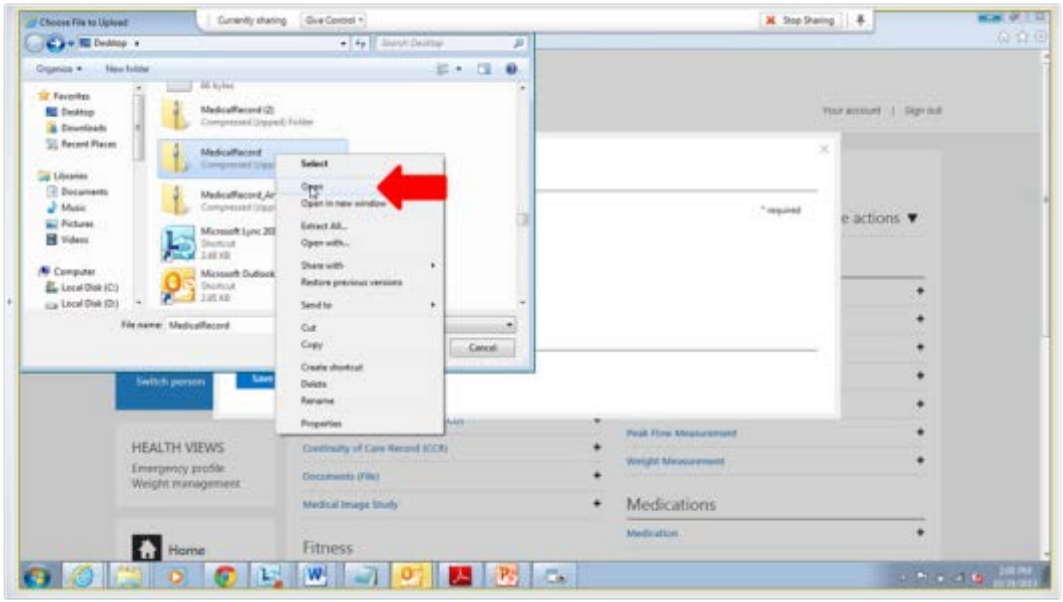
3) Now click **More actions** and choose **Upload a file** from the drop-down list.



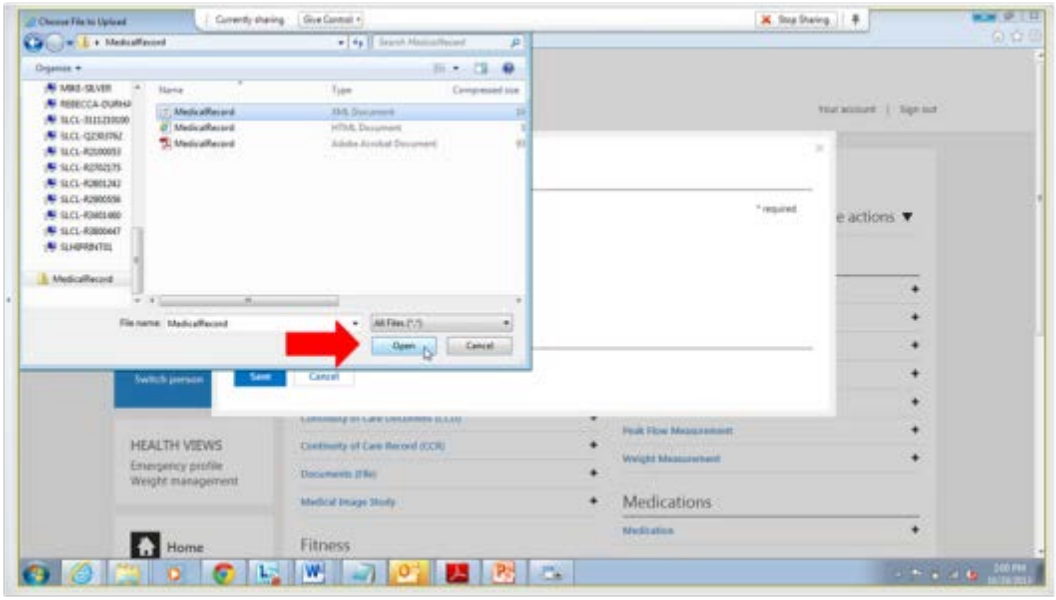
4) Click **Browse**.



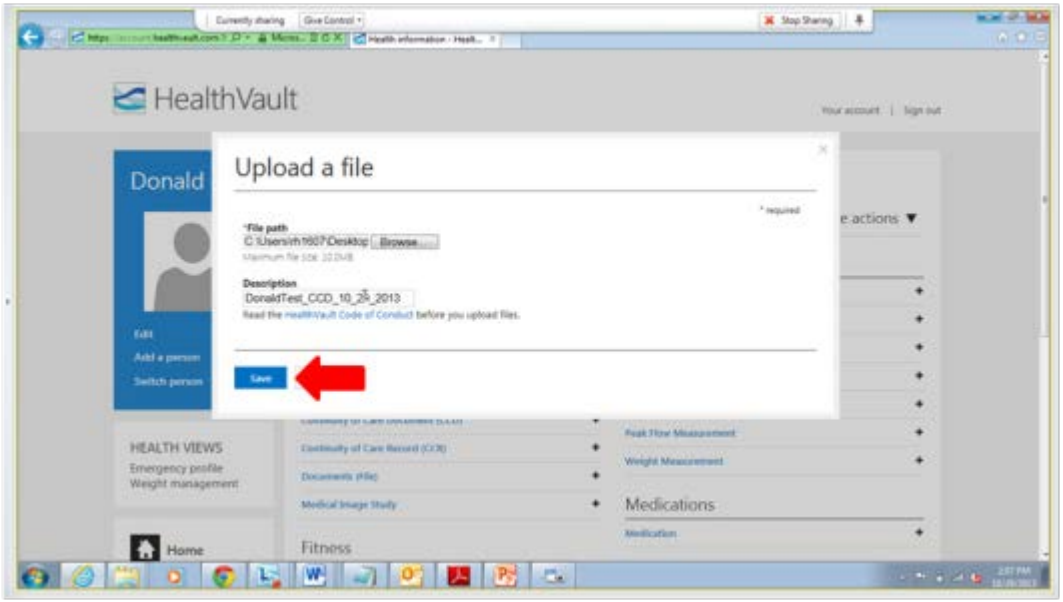
5) Right-click the folder where you saved your CCD and click **Open**.



6) You will see three files with the same name. Look at the Type column and click on the one with the file type XML Document and then click **Open**.

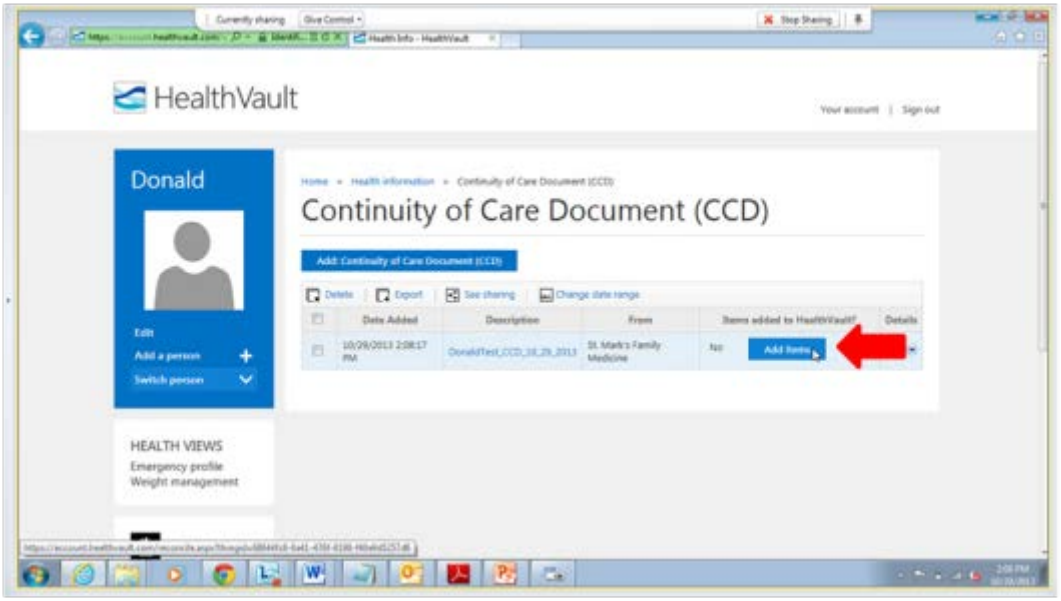


7) If you want, you can add a description of the file in the Description box. It's a good idea to include your name and the date. The file name and description can be the same. Click on **Save.**

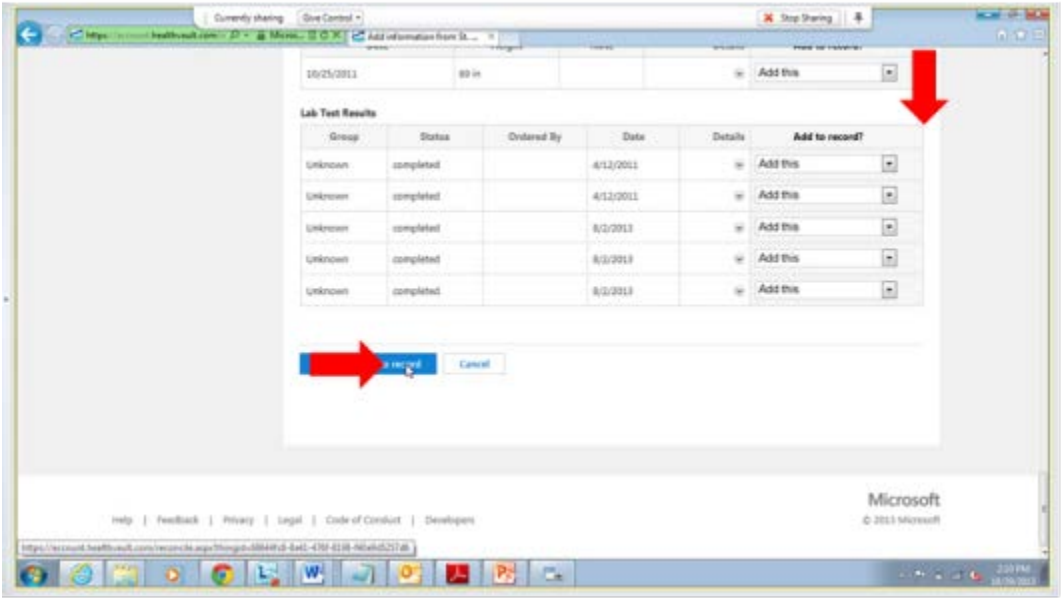


Optional step: Click on the **HealthVault Code of Conduct** to review it, especially the first time you upload a file.

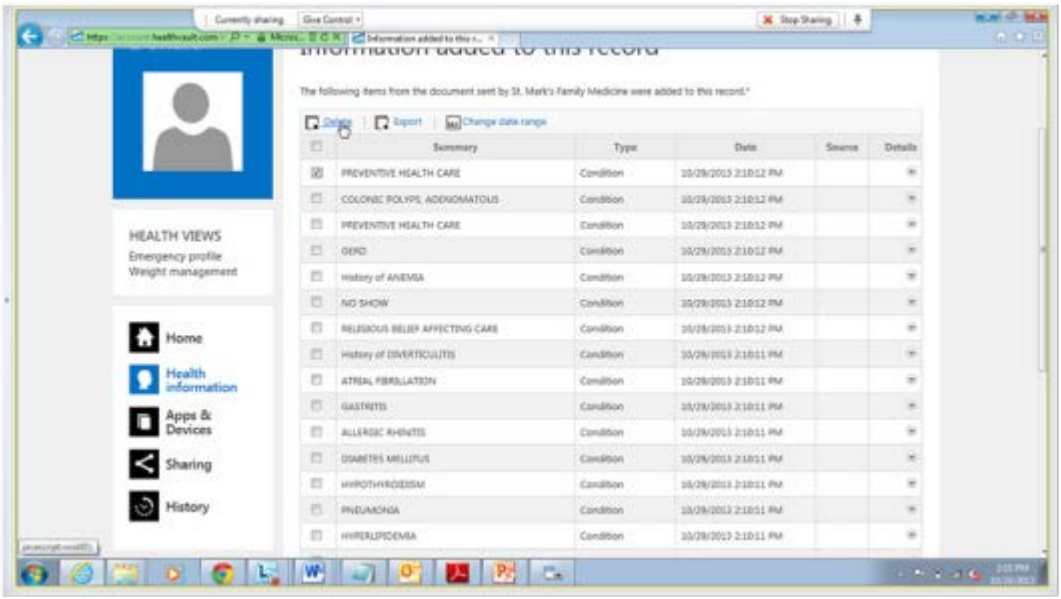
8) You will now be looking at the CCD page. Click **Add Items**.



9) Look at the "**Add to record?**" column. If there is something you don't want to add, change it by clicking the drop-down menu and selecting your preferred choice. Then click **Save changes to record.**



10) The next page shows you what has been added to your record. If you already uploaded some of this information from an earlier CCD, it will not be duplicated.



The information from your new CCD is now saved. No additional buttons to click.

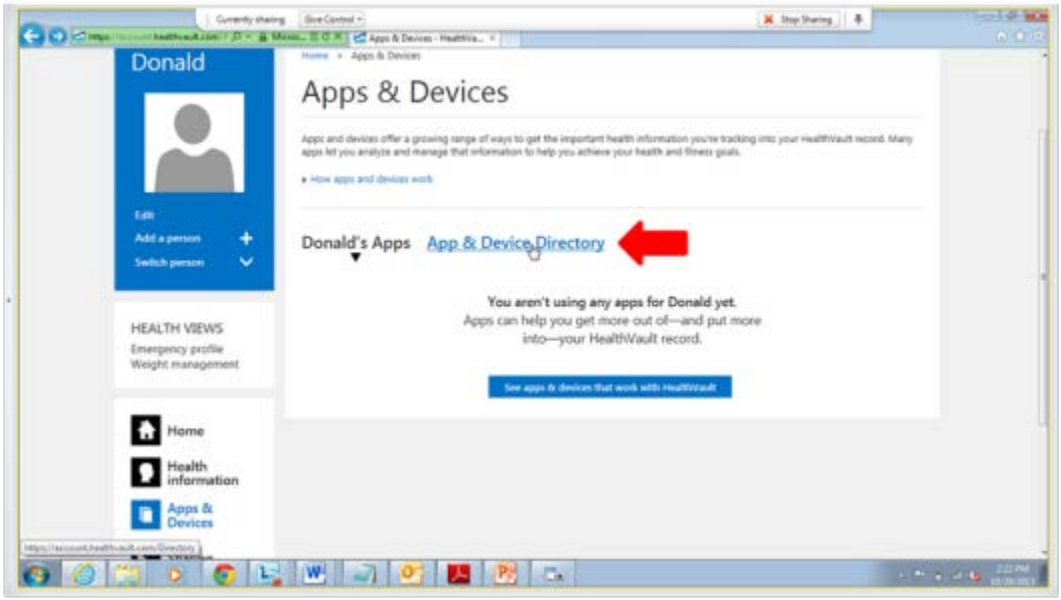
Optional Step: If there is anything you don't want to add to your HealthVault record, you can delete it here. Click the check box next to an item (do this for as many as you want to get rid of) and click **Delete**.

Set Up the HealthVault Connection Center

The HealthVault Connection Center will allow you to add information from devices. First we'll set up the Connection Center; then we'll connect a glucometer to HealthVault in the next section.

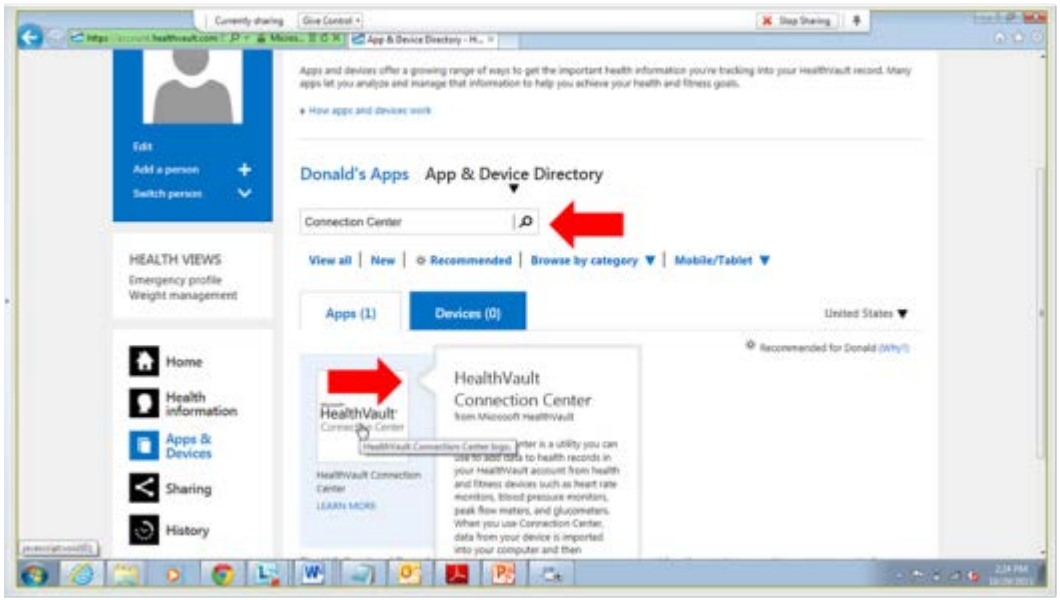
1) On the HealthVault homepage, click **Apps & Devices**.

2) Click **App & Device Directory**.

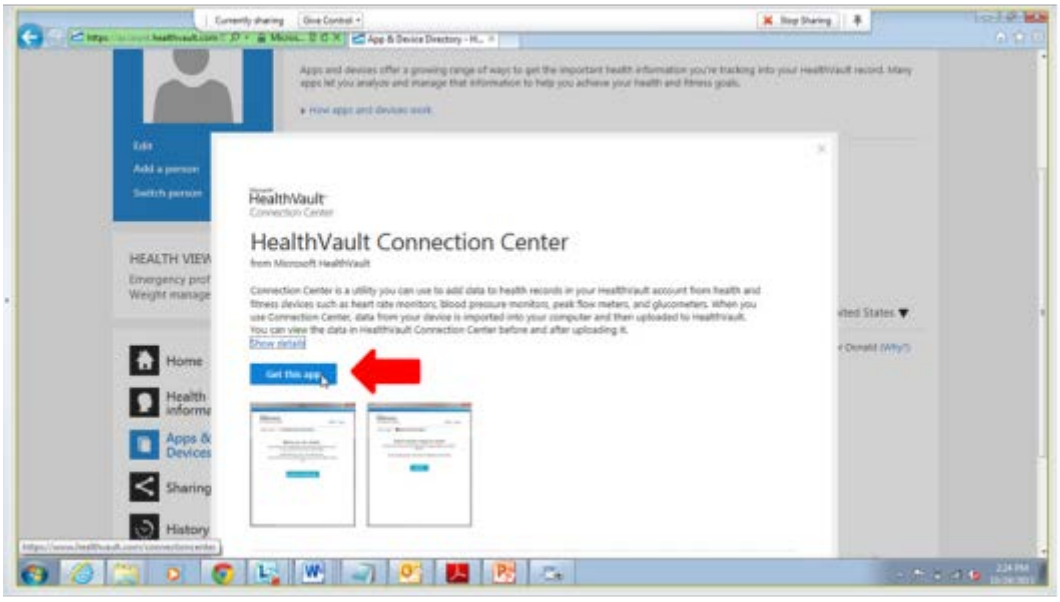


3) Type the words "connection center" into the search box and click the magnifying glass to search.

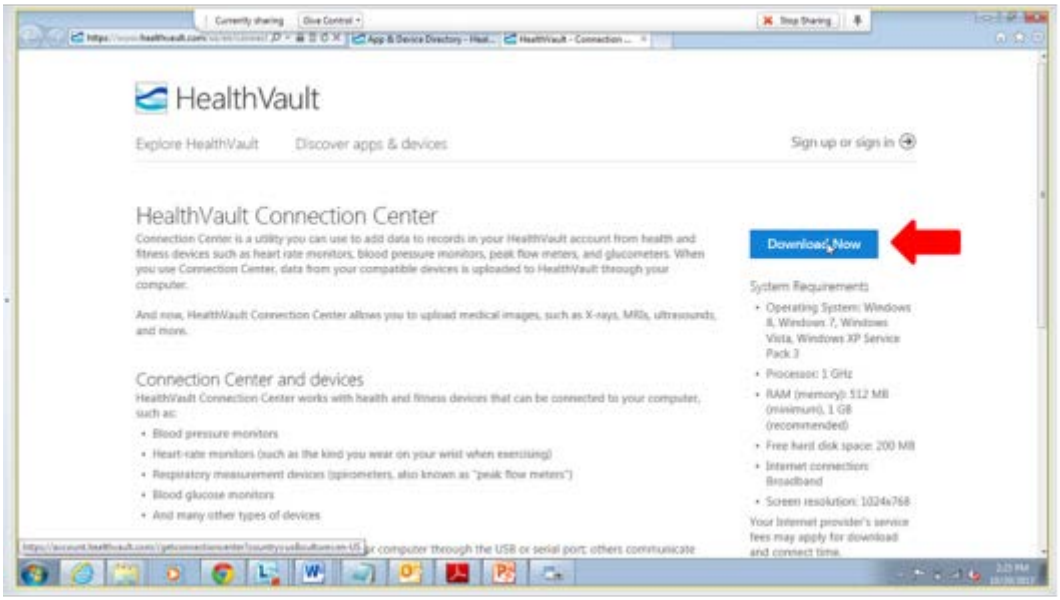
4) Click on the **HealthVault Connection Center**.



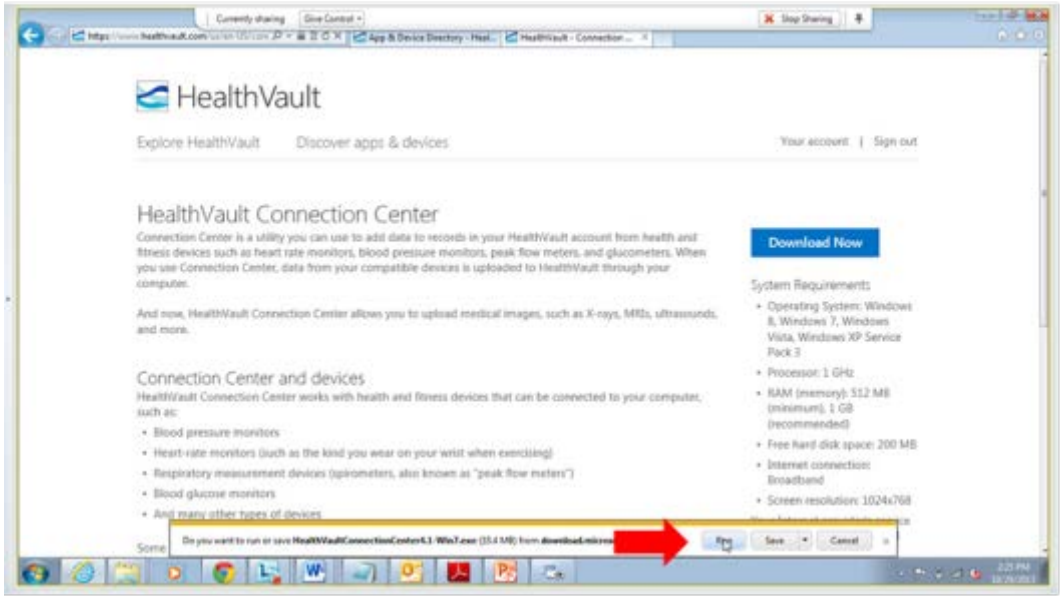
5) Click **Get this app** in the pop-up window.



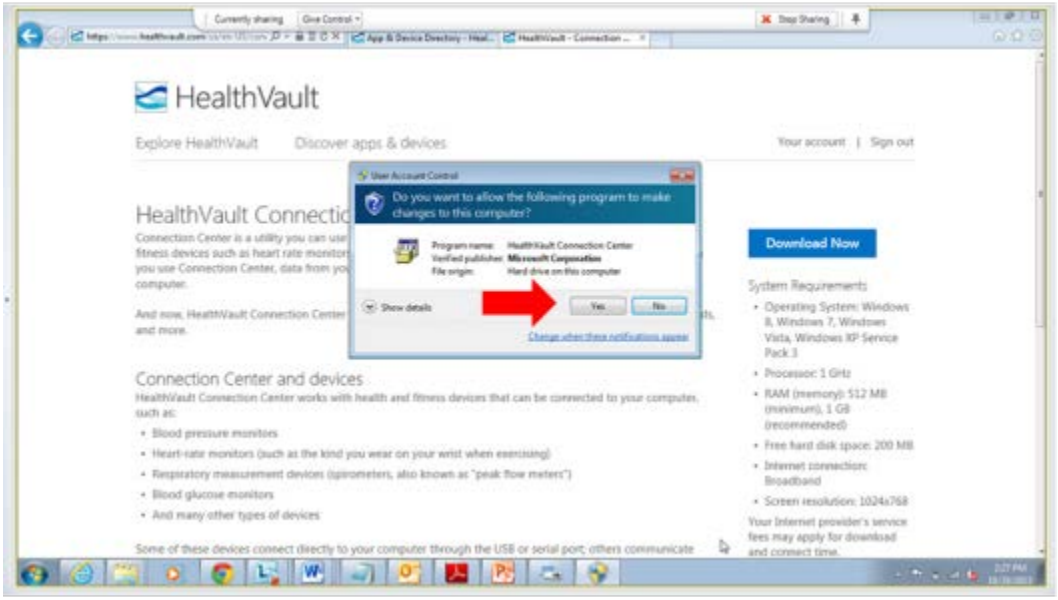
6) Click **Download Now**.



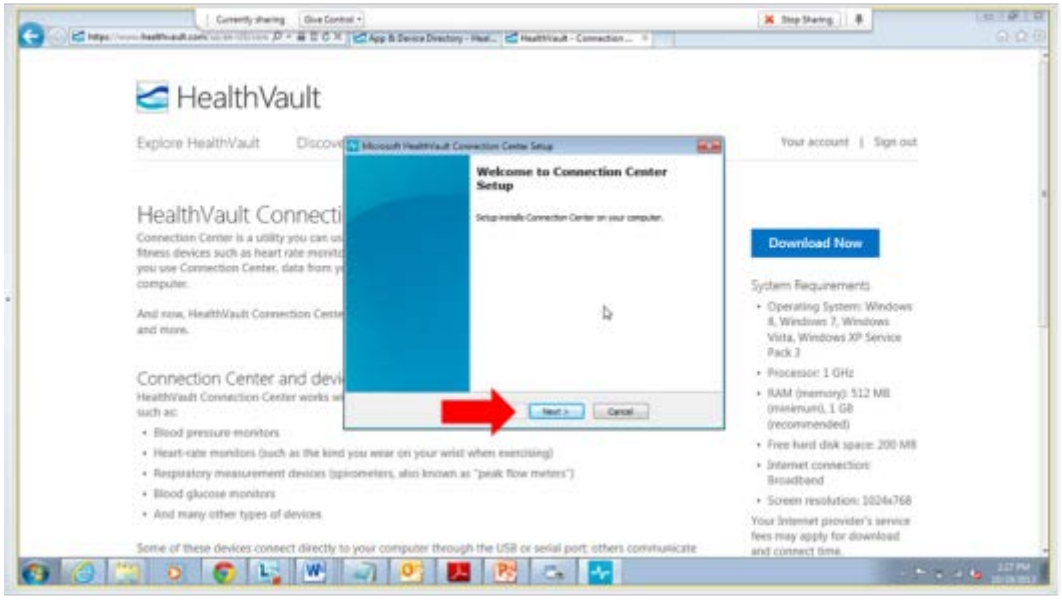
7) In the pop-up Download bar, click **Run**.



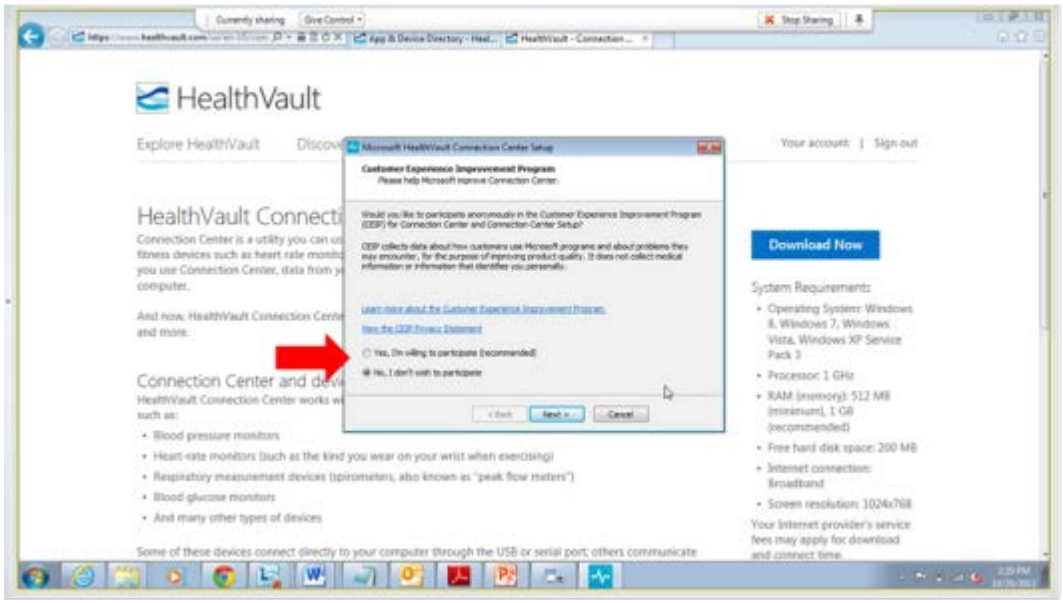
8) If you receive this security pop-up window, click **Yes**. The download will take about 3 minutes.



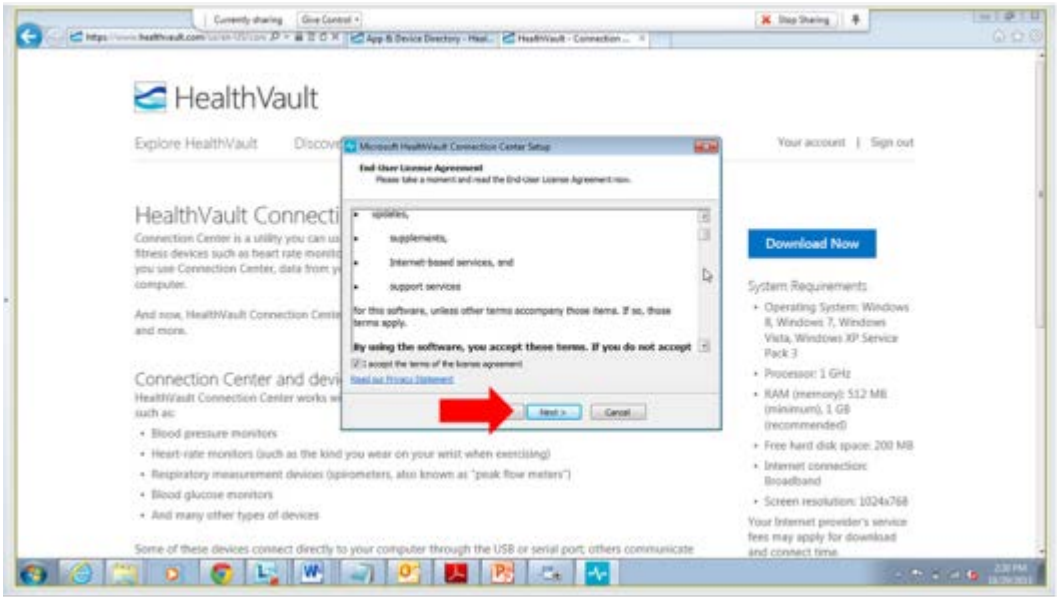
9) Click **Next** to start the installation.



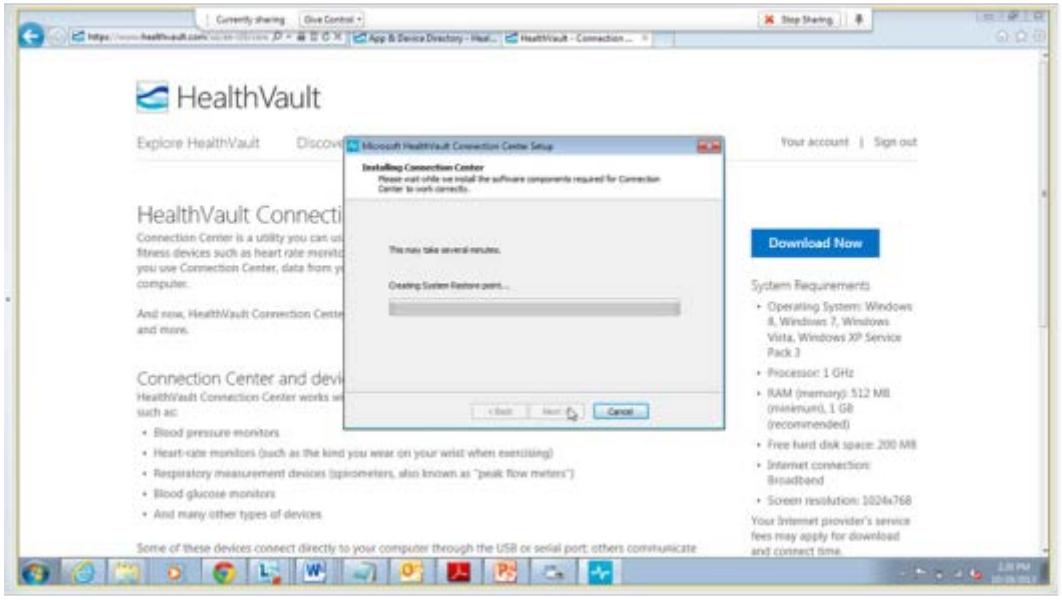
10) Choose **Yes** or **No**, whichever you prefer (either choice is acceptable).



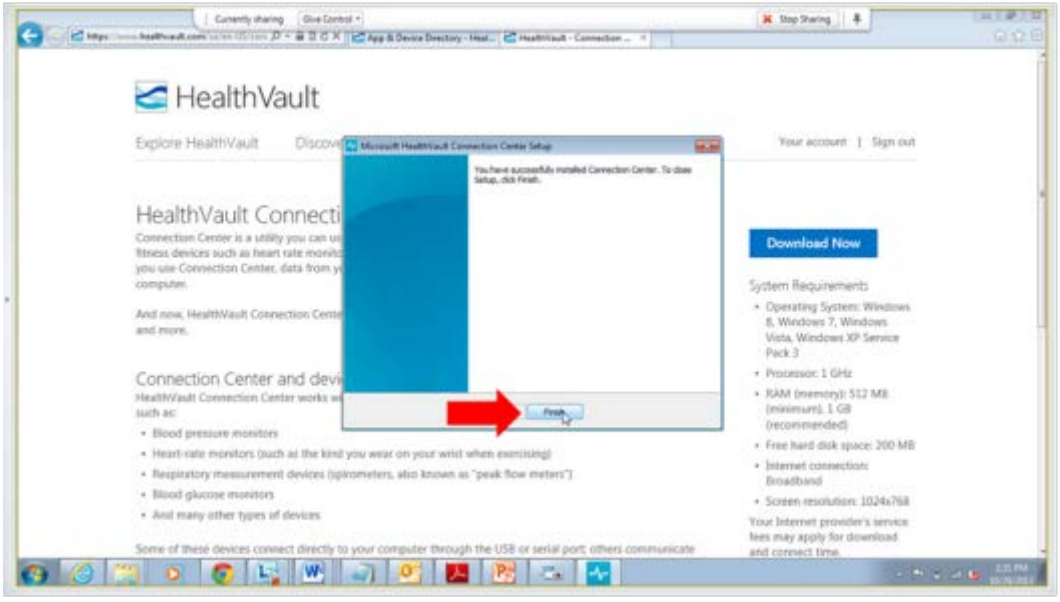
11) After reading the user agreement, check the box indicating that you accept the terms and then click **Next**.



12) You will see this progress bar. It may take a few minutes to install.



13) Click **Finish** to complete the installation.

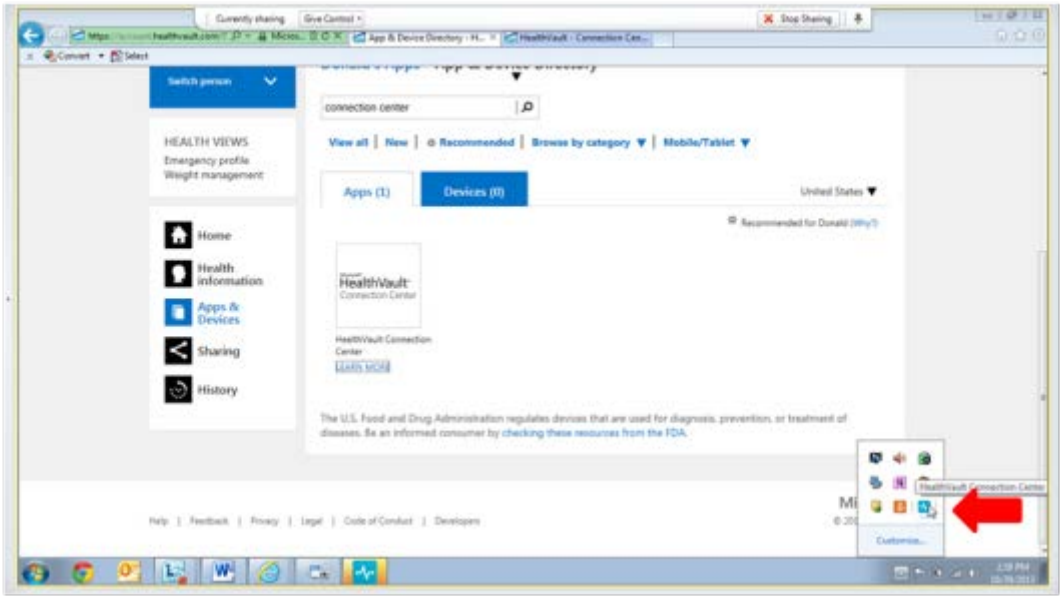


14) **Important**: Sign out of your HealthVault account and then sign in again.

Add Glucometer Readings to Your HealthVault Account

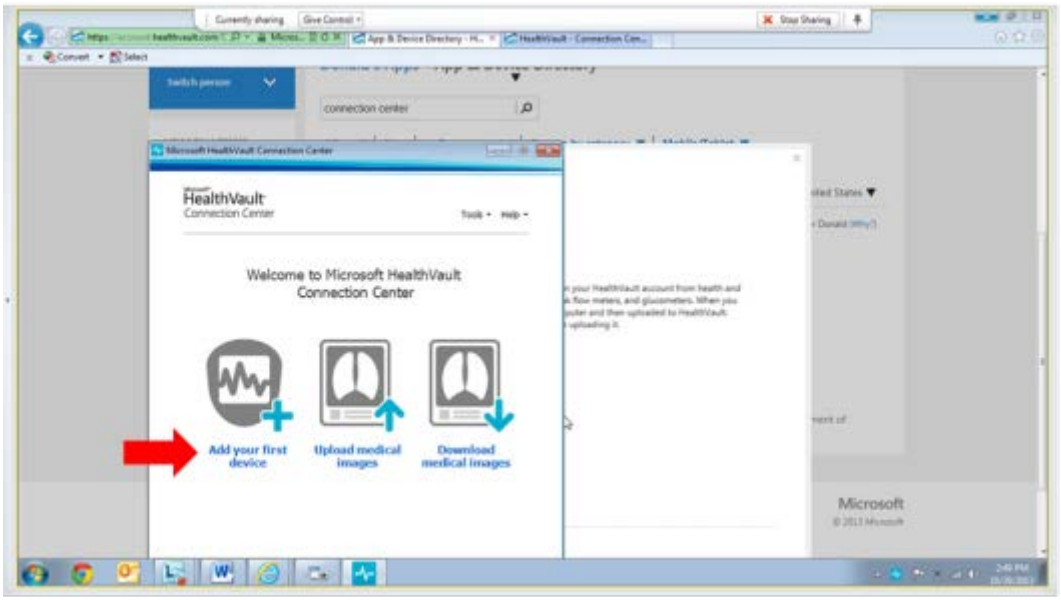
Now that the Connection Center is installed, you can connect devices to your PHR. This will let you see your readings over time and track your progress. The steps in this section may vary slightly depending on which glucometer you use.

1) In your computer task bar, choose the blue icon for HealthVault Connection Center.

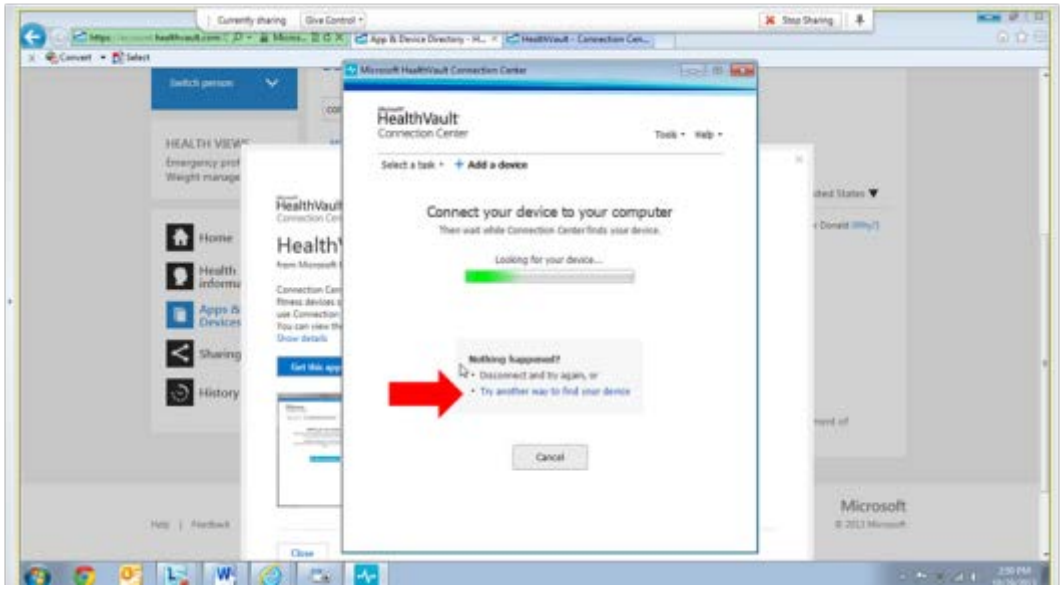


2) Take the cord and plug it into the glucometer and the computer. **DO NOT TURN ON THE GLUCOMETER**, even if the glucometer's instructions say to do so.

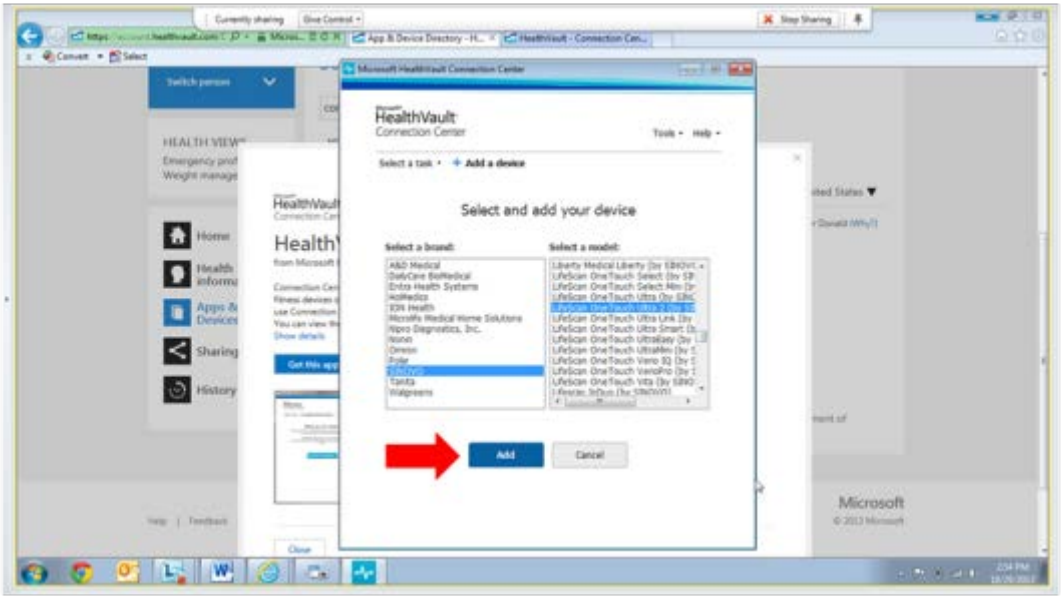
3) In the Connection Center window, click **Add your first device**.



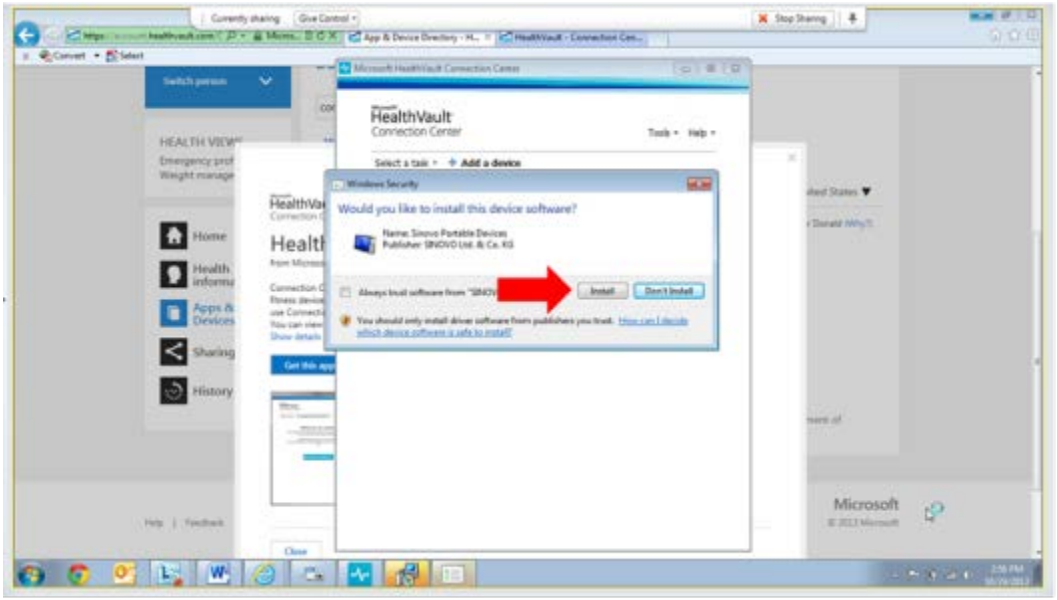
4) If your device appears, select it and skip to Step 6. If your device is not found, click **Try another way to find your device.**



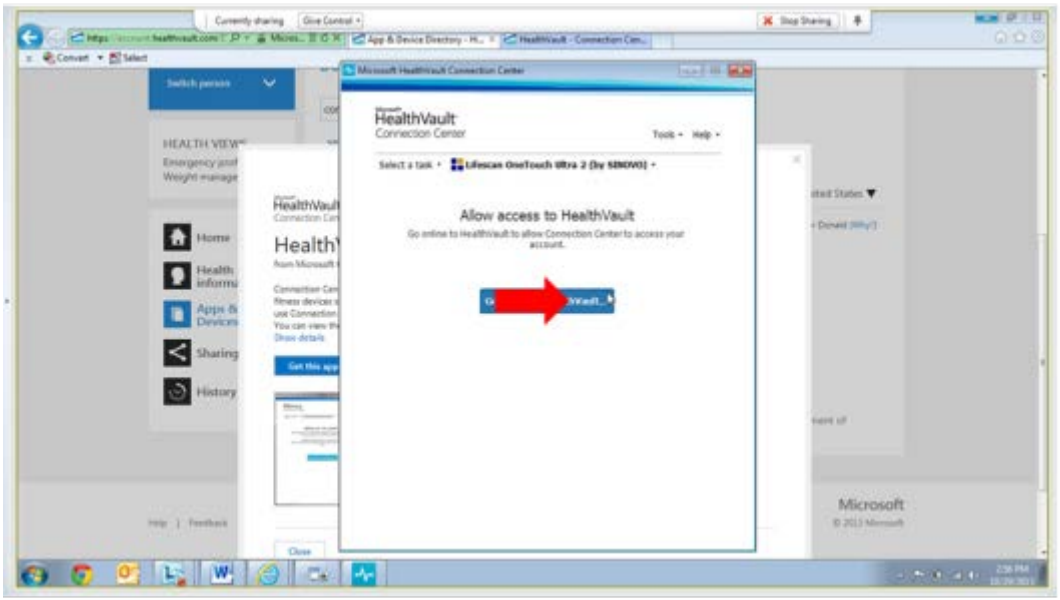
5) Select the brand of glucometer from the list on the left, and the type of glucometer from the list on the right. Click **Add**. (Note: Brand: **SINOVO**, Model: **Lifescan One Touch Ultra2**)



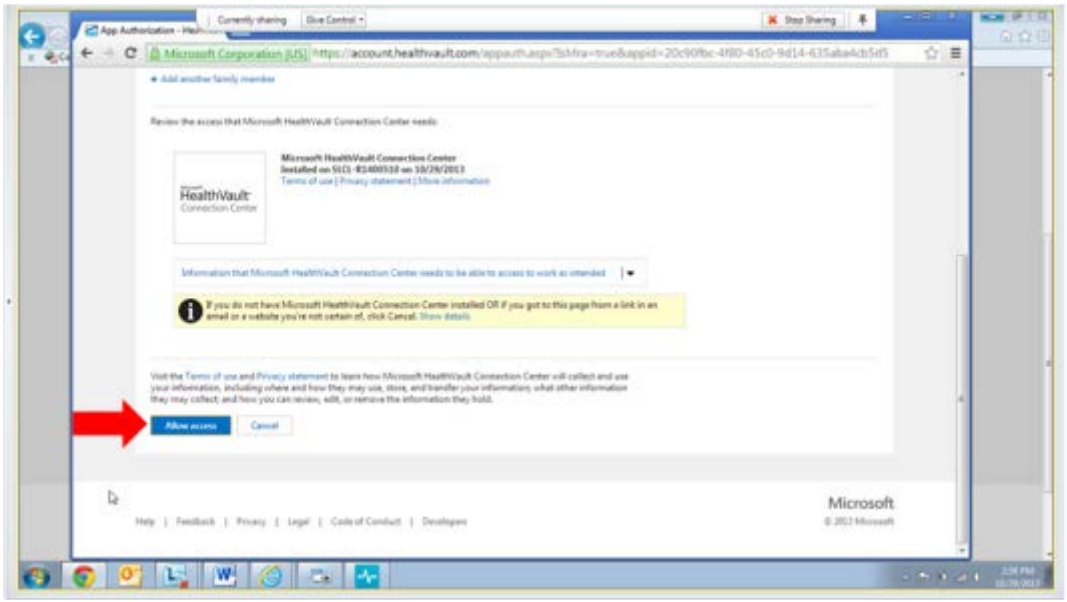
6) The Connection Center will download additional software for your device, click **Install** in the pop-up window.



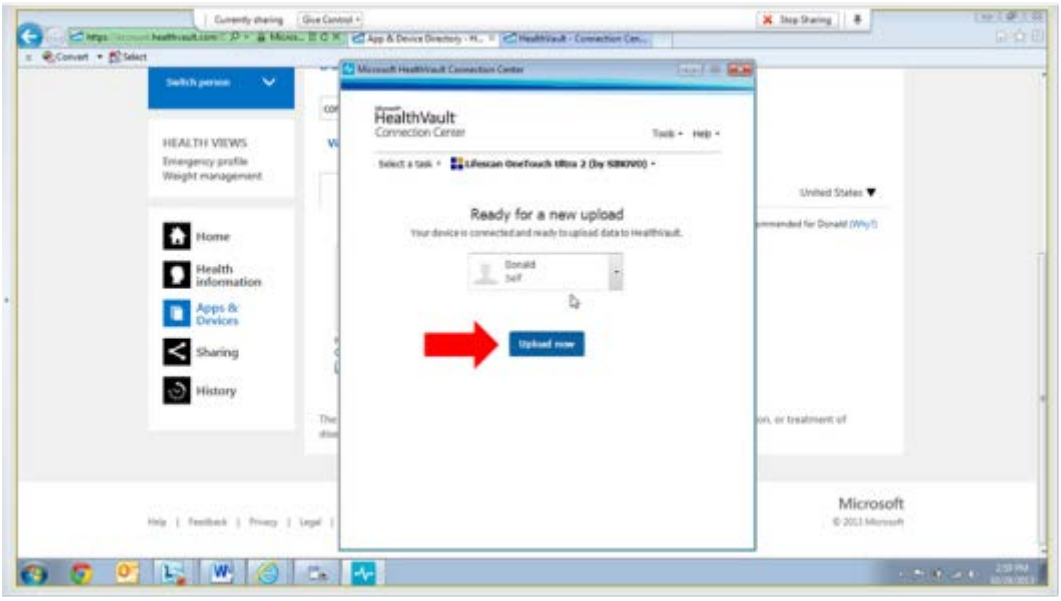
7) In pop-up window, click **Go online to HealthVault**.



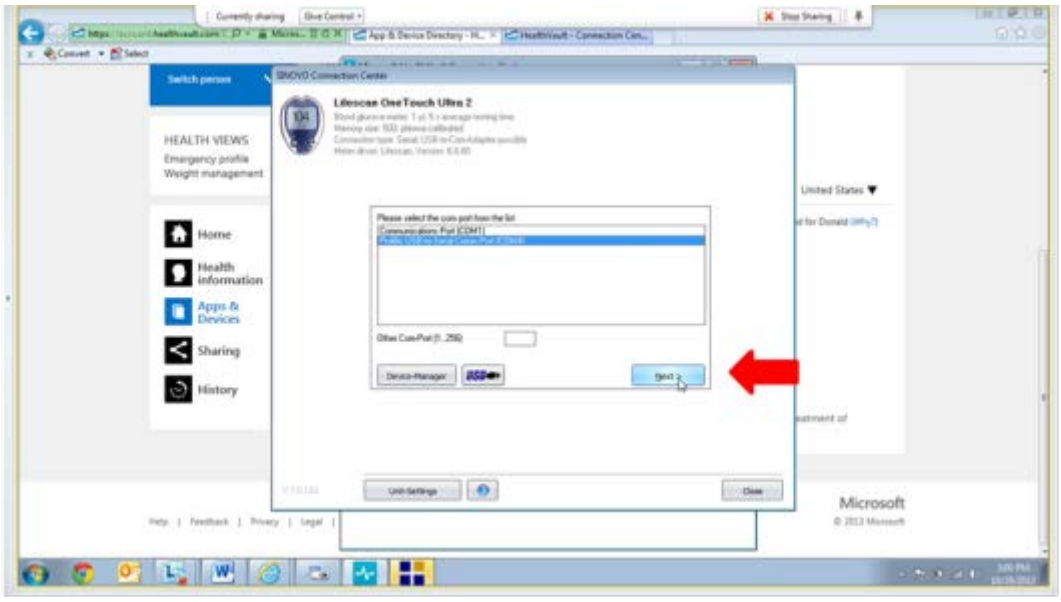
8) In the window that appears, click **Allow Access**.



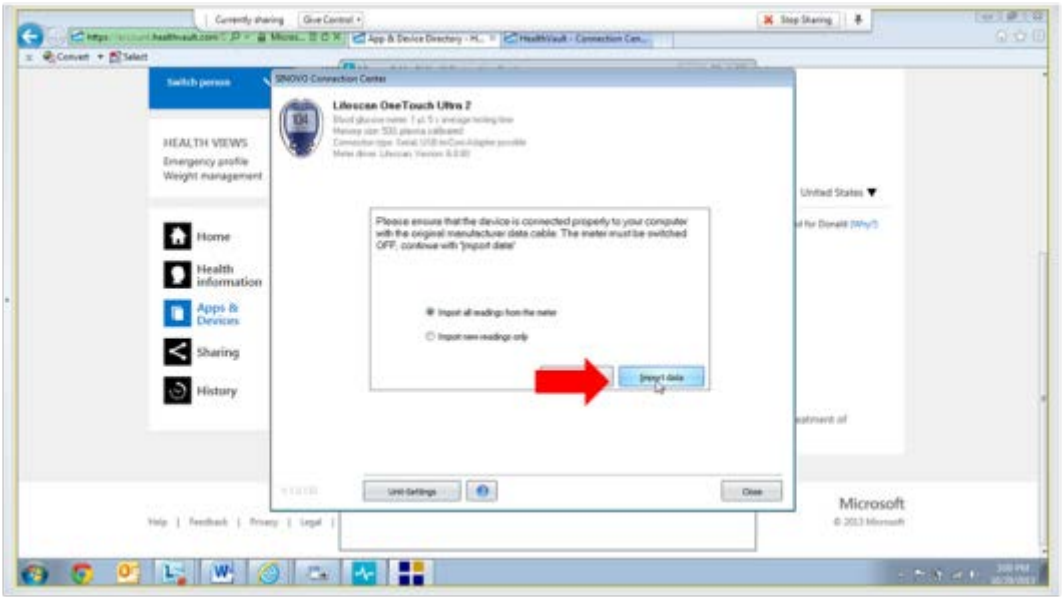
9) In the Ready for New Upload window click **Upload now**.



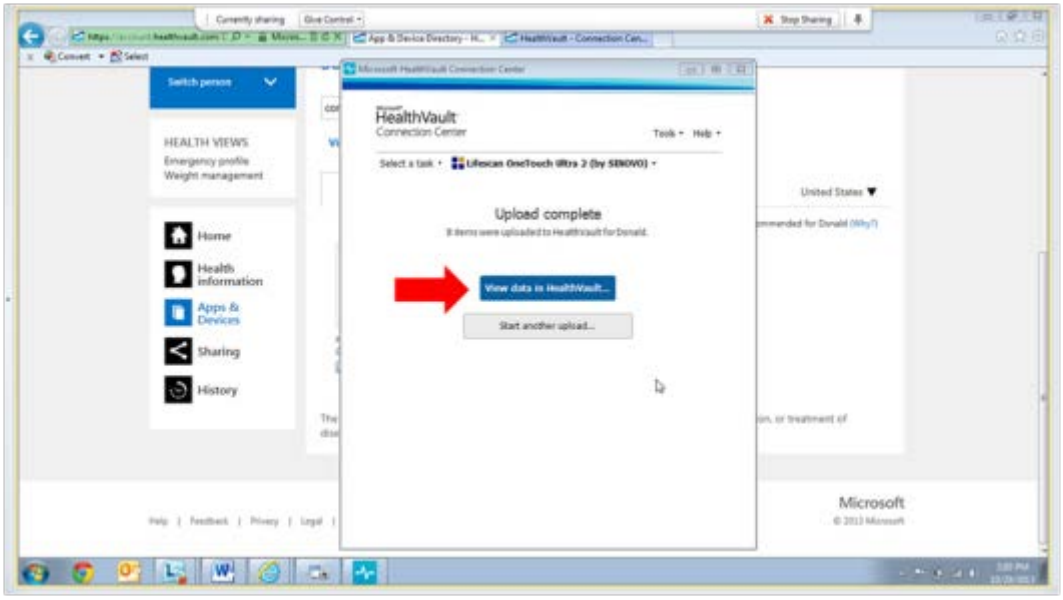
10) If you are asked to select a port, the default port selection should be correct. Click **Next**.



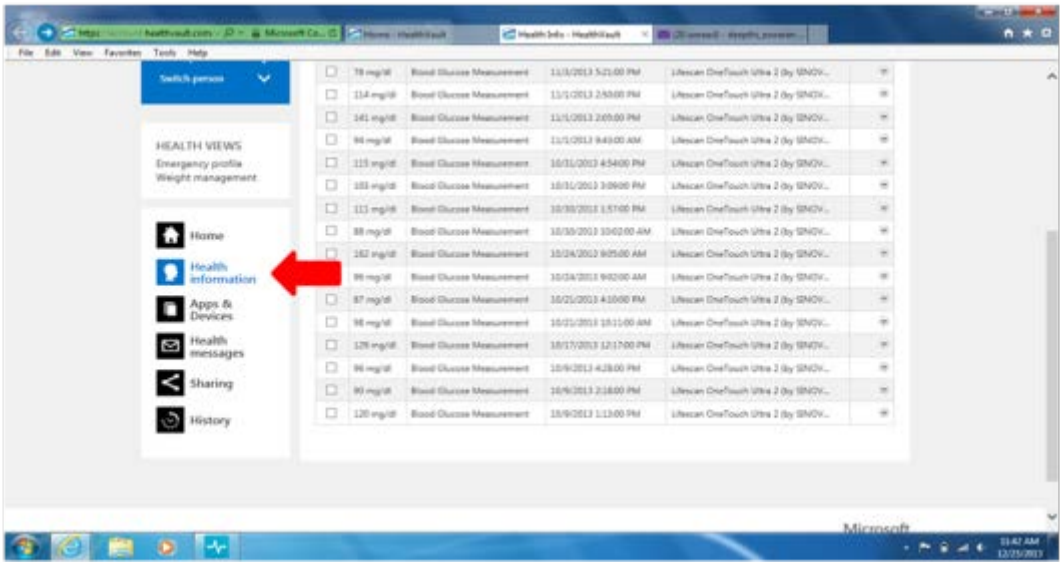
11) If this is your first upload, choose **Import all readings from the meter**. Otherwise, choose **Import new readings only**. Click **Import Data**.



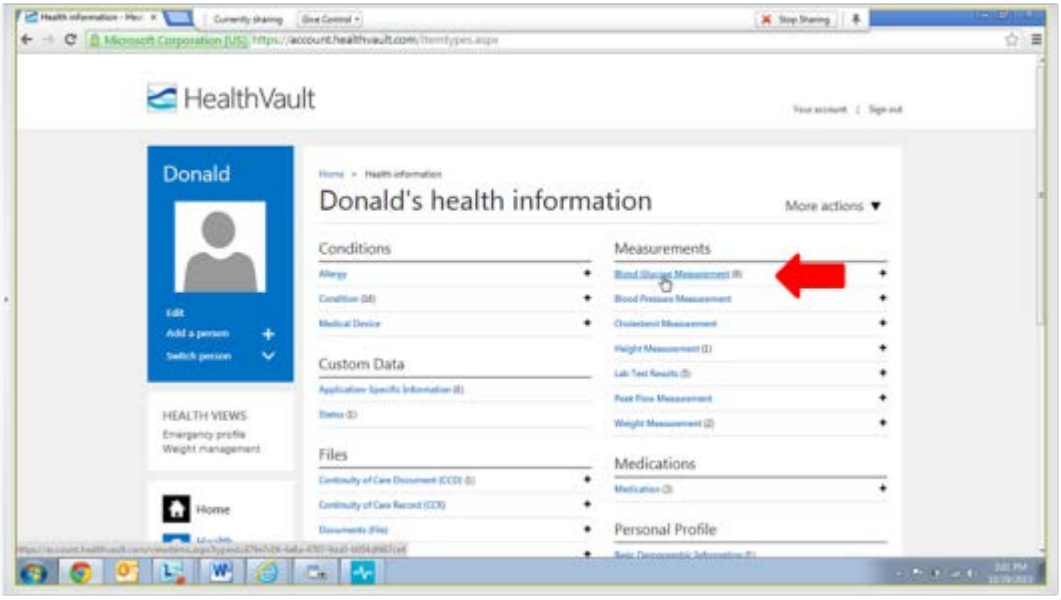
12) Click **View Data in HealthVault**.



13) Your information is now saved. Now click **Health Information**.



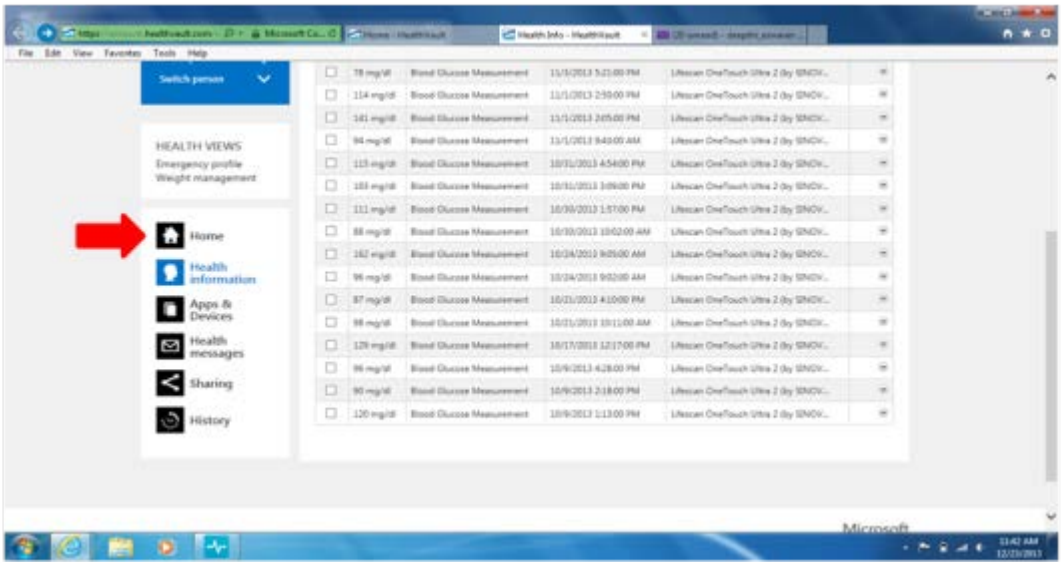
14) Under the Measurements section, click **Blood Glucose Measurement**.



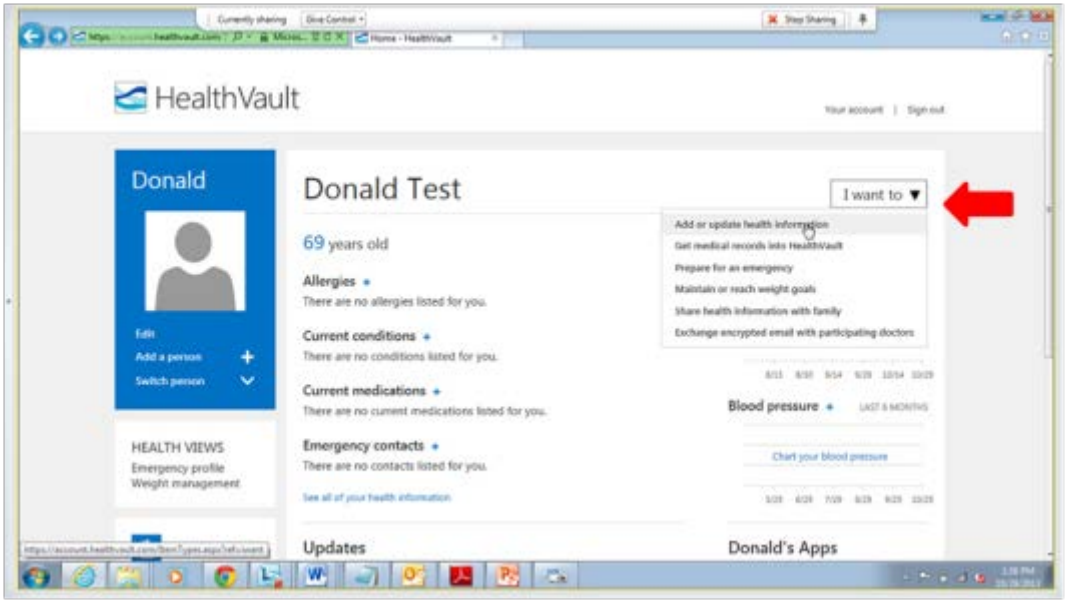
Send Your Health Information to Your Doctor

You have successfully created a more complete medical record in your PHR. Now let's send it to your doctor. Through HealthVault, we will use Direct email, which is different from your usual email. It is encrypted to be more secure. You can only exchange Direct email messages between two Direct email addresses.

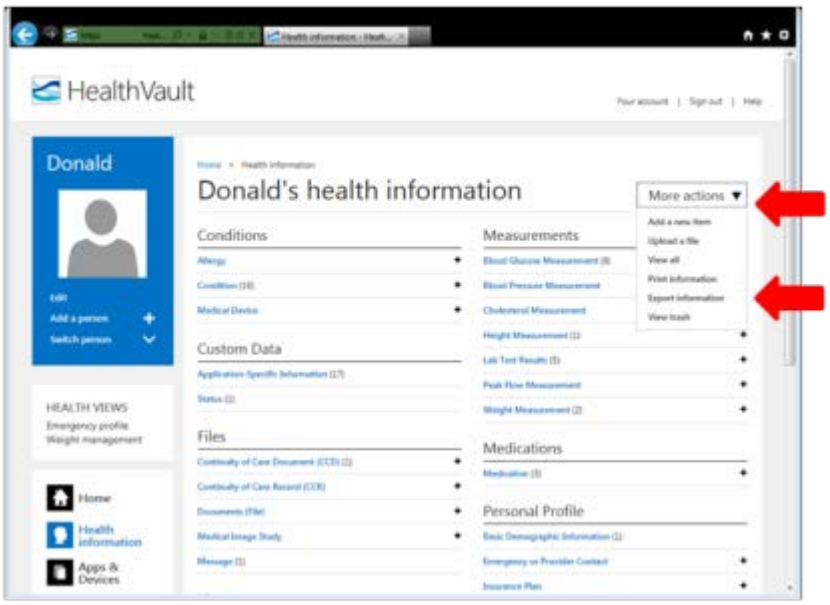
1) Go to the HealthVault homepage, click **Home**.



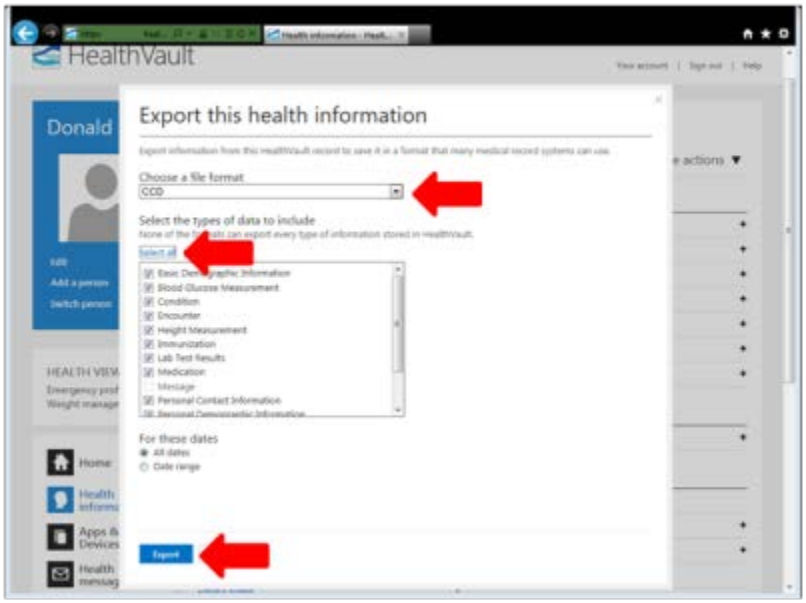
2) Click **I want to** and then choose **Add or update health information** from the drop-down list.



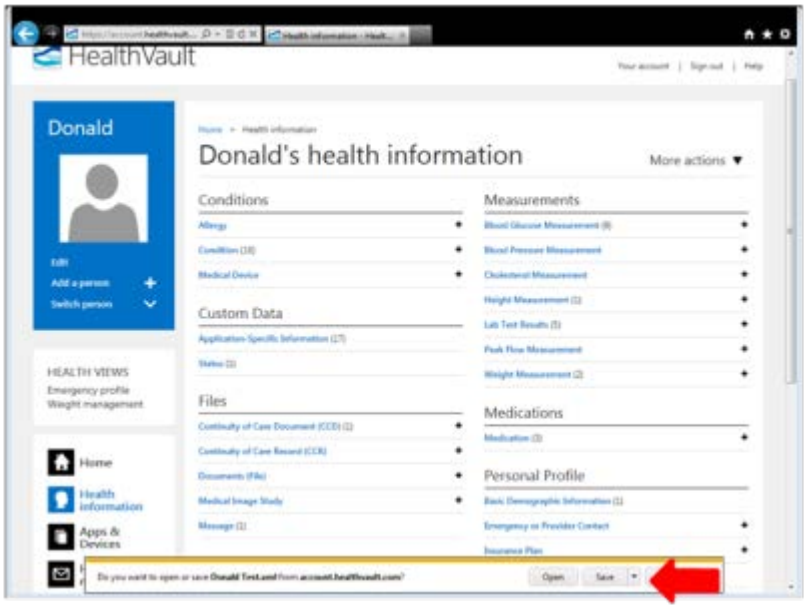
3) Click **More Actions** and then choose **Export information** from the drop-down list.



4) Set the file format to **CCD**, then click **Select All** under "Select the types of data to include", then click **Export**.

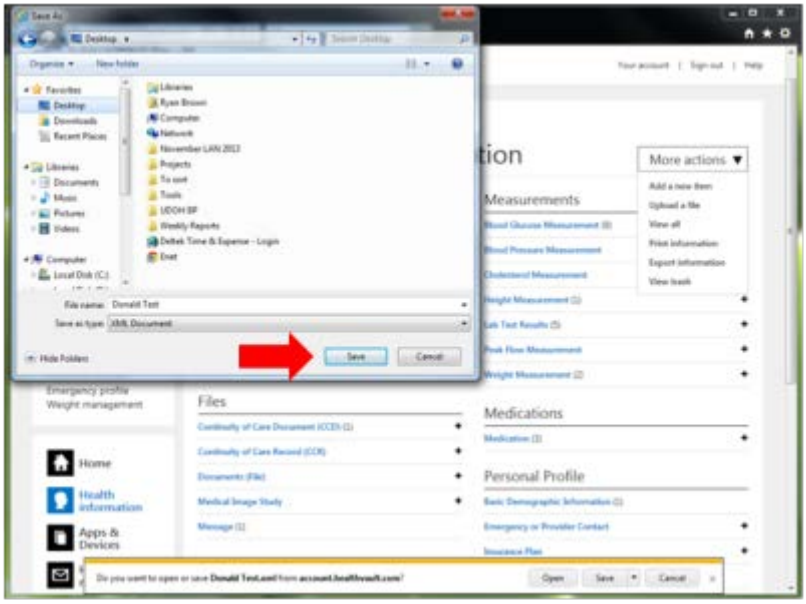


5) In the pop-up Download bar, click the small drop-down arrow next to the Save button and click **Save As**.



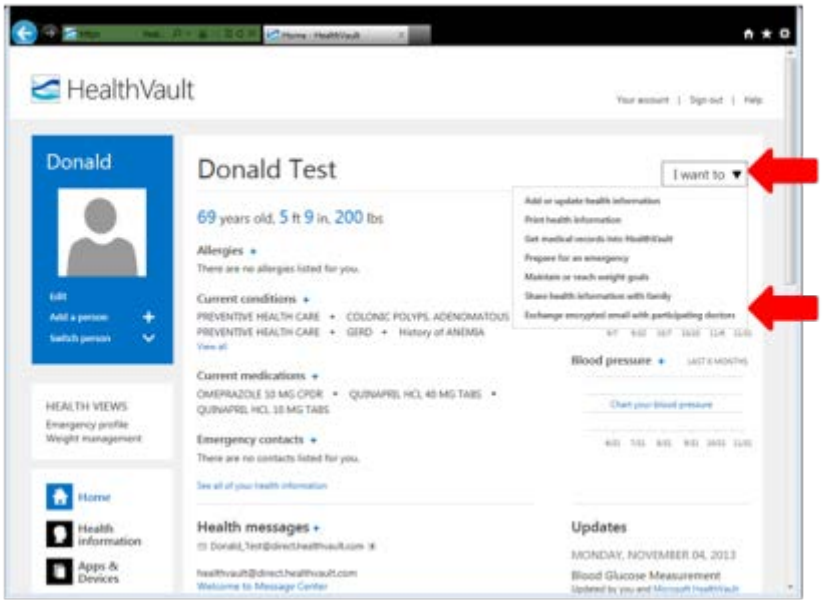
6) Choose a place to save the file. It's a good idea to save it on the Desktop with a file name that includes your name and the date, just like when we exported the CCD from your doctor's patient portal. For example, HealthVault_Donald_Oct2013.

7) Click **Save**.

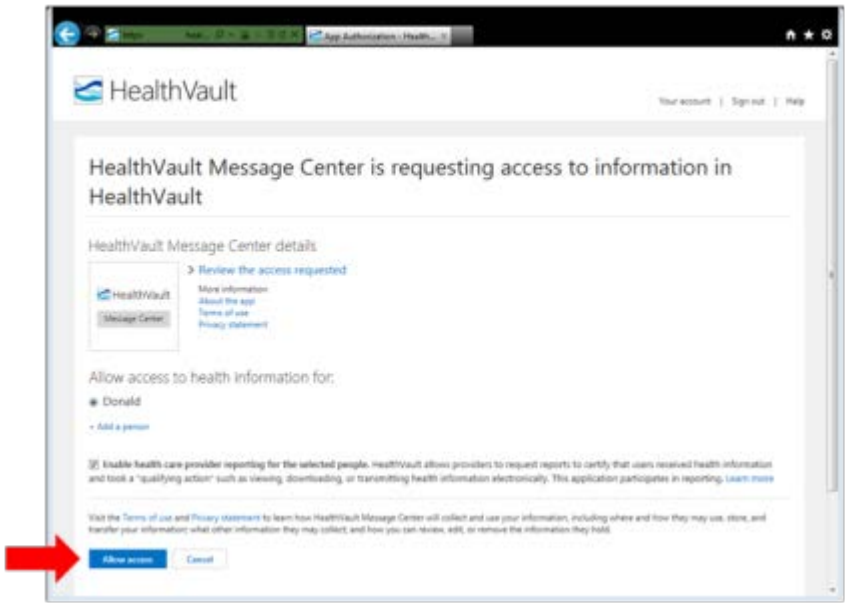


8) Go to the HealthVault homepage.

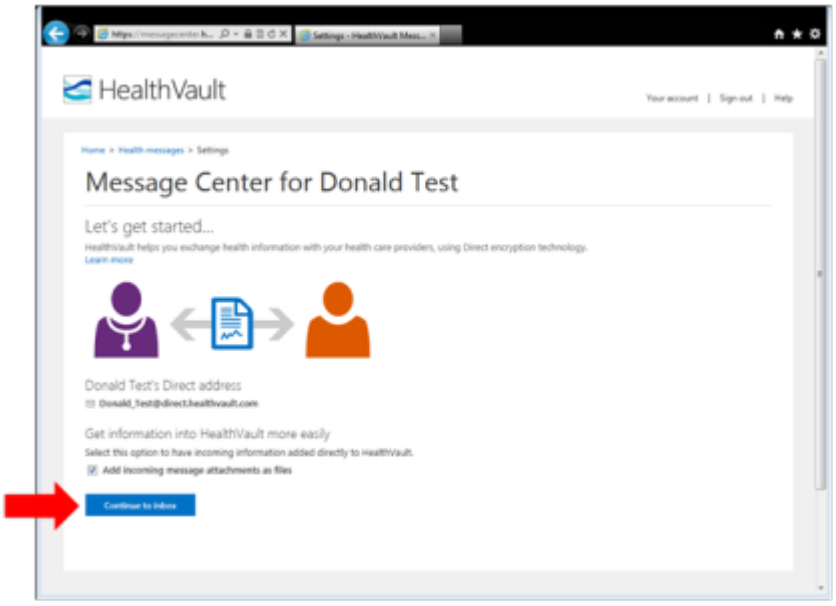
9) Go to **I want to** and select **Exchange encrypted email with participating doctors** from the drop-down list.



10) Click **Allow access**. This is for the HealthVault Message Center. (Similar to the Connection Center, the Message Center is an additional piece of software you need to do certain tasks.)

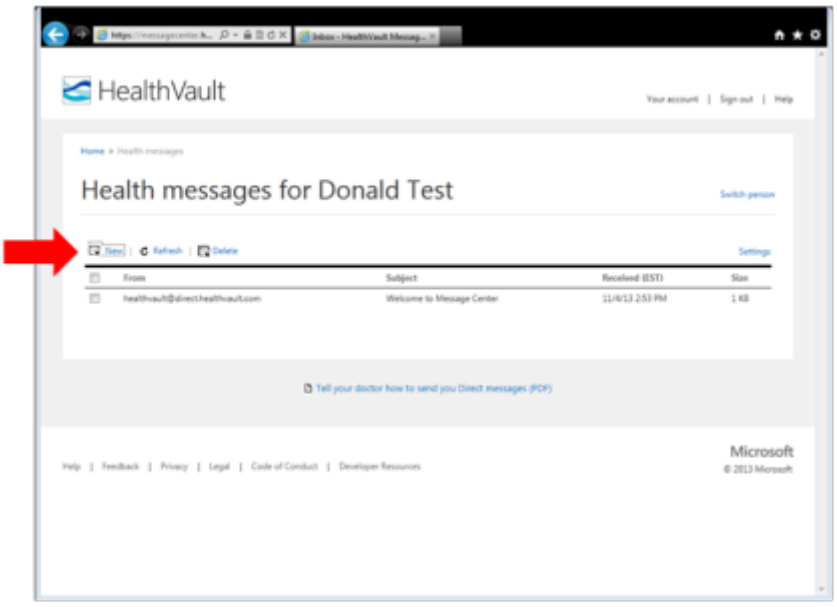


11) The first time you send an encrypted email you will be asked to set your Direct email address. If you want to change the suggested email address, change it in the box. Once you have a Direct email set up, your screen will look like this:

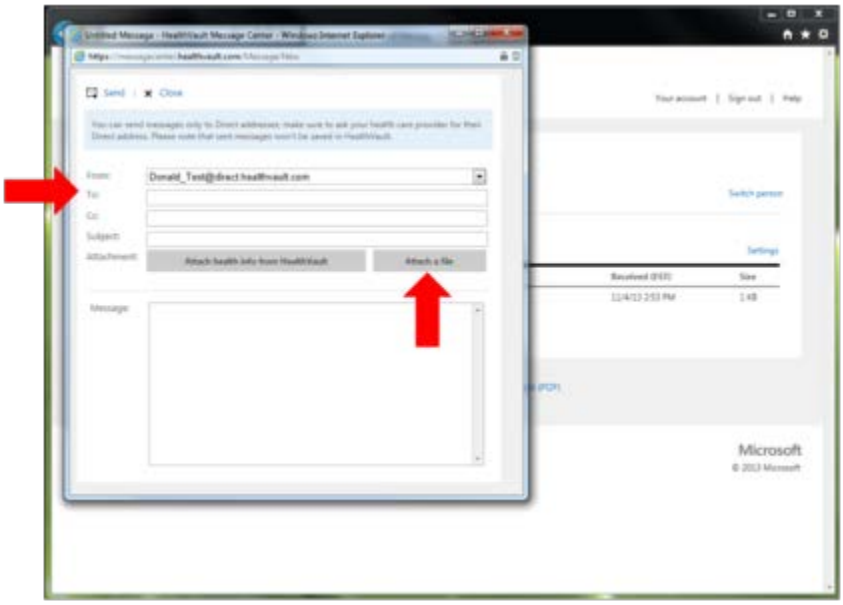


12) Click **Continue to Inbox.**

13) In the Inbox, click **New**.



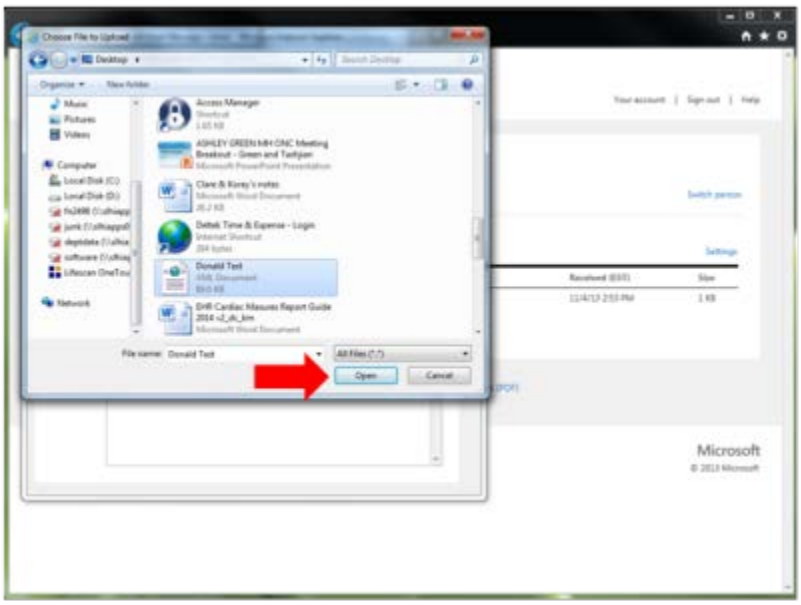
14) Insert your doctor's Direct email address in the To: field. It will look something like this: doctor@clinic.direct-ci.net. If you do not know your doctor's Direct address, call his or her office.



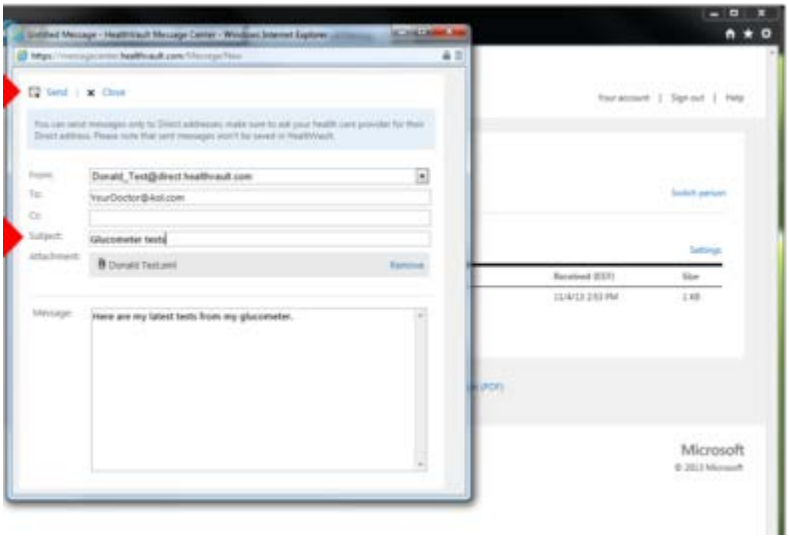
15) Click **Attach a file**, then **Browse**.

16) Go to the location where you saved your newly created CCD. Click on the file.

17) Click **Open**.



18) Add a subject and message to your Direct email.



19) Click **Send**.

Congratulations, you did it! Once you've been through the process once, there are a lot of steps you won't have to do again.

Be sure to update your record regularly. After an office visit or lab test is a good time, so you can check your progress and watch out for any mistakes in your record. Use your PHR to track your progress toward health goals. Tell your doctor how you are managing your health and share your information with him or her.

Contact Information

Deepthi Rajeev, PhD, MS, MSc
HealthInsight
Email: drajeev@healthinsight.org

Larry Garrett, PhD, MPH, RN
HealthInsight
Email: lgarrett@healthinsight.org

Clare Lence, MPH, MPP(c)
HealthInsight
Email: clence@healthinsight.org

Ryan Brown, MPH, MHA
HealthInsight
Email: rbrown@healthinsight.org

APPENDIX C
MEANINGFUL USE REQUIREMENTS THAT MAY BE MET BY PHRs

Stage 1 Meaningful Use requirements that may be met using PHR technology:

- **Core Set Requirements**
  - Having patients input their own demographic information
  - Providing patients with an electronic copy of their health information and discharge instructions via PHRs
  - Providing clinical summaries for patients for each office visit via PHRs
- **Menu Set Requirements**
  - Providing patients with timely electronic access to their health information. This requirement, with few exceptions, can only be achieved through the using a PHR technology
  - Providing patient-specific education resource via a PHR
  - Sending reminders to patients via their preferred PHR

Stage 2 Meaningful Use requirements that may be met using PHR technology:

- **Core Set Requirements**
  - Having patients enter their demographic information
  - Sending patient reminders via PHR technology
  - Having patients view, download, or transmit their health information via PHR
  - Providing clinical summaries via PHR
  - Providing patient-specific education via PHR
  - Having patients communicate with providers via secure messaging.
- **Menu Set Requirement**
  - Having patients input family health history via PHR.

[This page intentionally left blank.]