Kristen M Dunne. User Interfaces for Sharing Self-Generated Health Information in an SGHI Exchange Market. A Master's Paper for the M.S. in I.S. degree. December, 2013. 44 pages. Advisor: Robert Capra.

The goal of this project was to design a set of user interfaces to support a Self-Generated Health Information Exchange Market (SGHIx), in which users are given opportunities to share, and manage the sharing of, personal health information gathered from mobile health devices. The interfaces were designed such that the user is fully aware of what information he or she is sharing and with whom. The scope of this project included defining the use cases, designing the associated user interfaces, and then revising the designs after receiving feedback from the project stakeholders.

Headings:

Self-Generated Health Information

Health Information Exchange

mHealth

# USER INTERFACES FOR SHARING SELF-GENERATED HEALTH INFORMATION IN AN SGHI EXCHANGE MARKET

by

Kristen M Dunne

A Master's paper submitted to the faculty
of the School of Information and Library Science
of the University of North Carolina at Chapel Hill
in partial fulfillment of the requirements
for the degree of Master of Science in
Information Science.

Chapel Hill, North Carolina

December 2013

Approved by

_____

Robert Capra

# Table of Contents

# 1. Introduction

The goal of this project was to design a set of user interfaces to support a Self-Generated Health Information Exchange Market (SGHIx), in which users are given opportunities to share, and manage the sharing of, personal health information gathered from mobile health devices. The interfaces should be designed such that the user is fully aware of what information he or she is sharing and with whom. The scope of this project included defining the use cases, designing the associated user interfaces, and then revising the designs after receiving feedback from the project stakeholders.

Led by Tom Caruso, the SGHIx project is a joint effort of the School of Information and Library Science and RTI International's Center for the Advancement of Health IT. Self-generated health information (SGHI) is "information created, recorded, gathered, or inferred by or from individuals by a variety of mobile health (mHealth) applications and devices" (Caruso, 2013). Some common examples of this data may include daily step counts from Fitbit[1], GPS running data from a Garmin[2] watch, or calories tracked with MyFitnessPal[3]. There are a growing number of devices that track this type of data, and the SGHIx project aims to create a web application where individuals who use these apps and devices, and are thereby *information producers*, can exchange their information with various *information consumers*. The consumers may include health care providers, health researchers, or even the Center for Disease Control (CDC). The SGHIx would allow information consumers to offer something to the information producers in exchange for

[1] http://www.fitbit.com/
[2] http://connect.garmin.com/
[3] http://www.myfitnesspal.com/

sharing their data. This may be the opportunity to participate in a study, coupons for participating retailers, reward points, or even money. The details on this part of the Exchange Market have not yet been determined and are an item for future work. The current project used points to represent this reward in the interfaces that were designed. A concept image for the system can be seen in Figure 1 below, taken from a SGHIx project proposal presentation (T. Caruso, personal communication, September 20, 2013).


**Figure 1.** SGHIx Design

When a new information consumer, referred to as the "user" from here on, joins the SGHIx, they will first create an account. Once the account is established, the user will be able to upload their SGHI data. This can be done as often as needed to upload and/or update data from multiple mHealth devices. An information consumer may be interested in all of this data, or just specific pieces of it. For each set of data uploaded, the user must determine how much of it they are willing to share and with whom. The SGHIx should support a variety of user needs to control access to their data, but also make it clear and easy to understand and modify sharing preferences. For example, a user may decide that they wish to share their Fitbit steps data with anyone, as long as the data is only used in

an aggregate data set, where their data cannot be individually distinguished from the data of other people in the aggregate set. Another sharing option may be that they are willing to share their de-identified data, meaning that the consumer would be able to see each individual data point without being able to know who the person is. A more conservative option could be that a user requires that an explicit request be made each time a consumer wishes to use their data. Each of these options is detailed in the Use Case Descriptions section of this paper. A user may select a general setting, but they should be able to change the setting at any point. Additionally, the user should be able to monitor the use of their data. These requirements present challenges for designing the user experience and were the motivation for this project's focus.

Given that the data shared within the SGHIx is personal health information, the system should make sure to follow any regulations regarding Protected Health Information (PHI). The Health Insurance Portability and Accountability Act (HIPAA) specifies privacy and security regulations for this type of data, to protect individuals. The details of HIPAA and PHI and how the SGHIx should compensate for them are outside the scope of this project. This project assumes that the system handles these specific regulations and focuses instead on the user experience and ensuring that the users understand how their data is being shared within the system.

The scope of this project included defining the use cases, designing the associated user interfaces, and then revising the designs after receiving feedback from the project stakeholders.

## 2. Related Work

There are several areas of research related to this project, covered in the literature review below. Topics include privacy concerns related to the sharing of information in electronic health records (EHRs), Health Social Networking Sites (HSNS), and other sites with mHealth data, as well as privacy controls of existing systems such as Facebook. Some research has been done on the interface design and usability aspects of these types of systems, which is covered as well.

In their viewpoint article, Yasnoff and his colleagues (Yasnoff, Sweeney, & Shortliffe, 2013) discuss how the use of EHRs can be successful. They note that in addition to complete records for patients, there must be a way to exchange that information, which they refer to as health information exchange (HIE) (p. 989). This is similar to what the SGHIx attempts to do. They discuss the discouraging lack of progress with the current HIE and contribute it to the wrong approach being used. Current systems are trying to replicate the existing process of paper records, where data is stored at each organization, making the process of exchanging data difficult (p. 989). Instead, they propose the use of patient-centric community health record banks (HRBs). "Health record banks are community organizations that put patients in charge of a comprehensive copy of all their personal, private health information… The patient explicitly controls who may access which parts of the information in his or her individual account" (p. 990). This puts the patient in control of the sharing, thus reducing the number of organizations that need to be involved in the information exchange process. The idea of people controlling access to their own data is central to the SGHIx system.

Also looking at EHRs, or electronic medical records (EMRs), Caine and Hanania's (2012) research examined which information in an EMR patients were willing to share, with whom, and for what purpose. Based on a questionnaire, card sorting exercises, and a semistructured interview of 30 adults, they determined that none of their participants wanted to share all of the information in their EMR with all recipients (including people and groups such as physicians, government agencies, health insurance companies, researchers, and family and friends). Instead, participants want granular control over sharing. What is shared depends on how sensitive the data is and who the recipient is. In general, people were more likely to share more information with their primary care physician and specialists than they were to share with research organizations, insurance companies, and even family members (p. 12). Their findings may suggest that users of the SGHIx system might also prefer to have similar granular control over the data that they share. One limitation mentioned with this study is that they did not use personalized patient EMR data for the card sorting task, meaning that results may be different if the participants were considering sharing their own data, rather than hypothetical data.

Weitzman, Kaci, and Mandl (2010) surveyed 151 early adopters of a live personally controlled health record (PCHR) system regarding the conditions under which they would share their information with for health research. Though participants were only asked hypothetically about sharing with research organizations specifically, several of their findings still apply to the SGHIx system. They found that 91% of participants were willing to share their data for research. Sharing was contingent on receiving an explanation of benefits and risks as well as customization of access controls in terms of

both granularity and time-limited restrictions (p. 6). Guaranteeing strict anonymity would increase sharing (90% of participants) but guaranteeing privacy but not anonymity would decrease willingness to share (71% of participants). Additionally, a means for viewing an audit trail of access to health information and a specific summary of shared data would also increase willingness to share (79% of participants) (p. 7). Somewhat surprisingly, only 29% of participants reported that payment for health information would increase their willingness to share. Even though this study focused only on health research organizations as the information consumers, the system is still similar to SGHIx and should likely apply to additional types of information consumers. The SGHIx system should implement access controls, guarantee anonymity where possible, and provide an audit trail for shared data.

Another area where personal health information is shared includes health social networking sites (HSNS). In his recent article, Li (2013) examines the privacy concerns within these websites. Primarily he notes that in the US, EHRs are legally protected, meaning sensitive data cannot be revealed to unauthorized parties, by the HIPAA privacy rule and the Health Information Technology for Economic Clinical Health (HITECH) Act, but that when users voluntarily post similar data on HSNS, their privacy is not protected by the HIPAA and HITECH acts (p. 704). Therefore he examines the associated privacy risks and discusses considerations for privacy policies. He mentions that "empirical and theoretical research suggest that users often lack enough information to make privacy-sensitive decisions and, even with sufficient information, are likely to trade-off long-term privacy for short-term benefits" (p. 705). Therefore, he identifies

privacy awareness and education as an important part of a privacy framework. This is an important factor to consider in the design of the SGHIx, where users will be sharing similar types of information, though in a more structured manner than may be encountered in HSNS. Specifically, the enticement of earning rewards for sharing information in the SGHIx could impact users' decisions to share their information. The user interface should ensure that the user is presented with all relevant information without being distracted by any benefits.

In their study, Prasad and his colleagues (Prasad, Sorber, Stablein, Anthony, & Kotz, 2012) explored the privacy concerns of sharing mobile health (mHealth) data such as data collected from a wearable sensor device. Rather than using hypothetical data as found in most other studies, they instead had users share their own data. This makes the results more valuable since other studies have discovered that what people say they would do is not always reflective of their actual sharing behavior (p. 117). For their study they had 41 participants, including college students, working adults, and retirees, each wear a Fitbit for five days, which tracked calories burned, steps taken, distance traveled, and sleep quality. The participants uploaded their data to a custom web interface each day and made sharing decisions about what to share with whom. In addition to the data from the Fitbit, the following traits could also be shared: age, gender, height, weight, health goals, overall activity level, and academic major (p. 118). Participants could choose to share information with family members, friends, and specific third parties such as academic researchers, medical labs, private companies, and the government (p. 119). The default setting was to share at the finest detail and participants had to "opt-out." Though the

requests to share with third parties used names of real organizations, the participants did not know that the requests were fake and that their data would not actually be exposed to the public. Their study revealed three main findings about people's privacy concerns. First, participants were less willing to share the additional traits about them than the data that was collected by the Fitbit. Second, participants shared more information with strangers than their own family and friends or the public, and were more willing to share their data if there were perceived benefits. Third, the study confirmed that privacy concerns are not static (p. 124). From these findings, Prasad and his colleagues provide two recommendations, "flexible controls need to support both fine- and coarse-grained approaches to sharing" and "reducing disconnect between information and granular controls" (p. 124). These findings are highly relevant to how the sharing settings within the SGHIx system should be designed. Users should to be able to easily see their data and change the sharing settings at any point.

Another area of research is that which examines the sharing controls of existing systems. Though the data shared on Facebook may not be mHealth data specifically, users do still share potentially private information. One study which examines the privacy controls in Facebook was done by Egelman, Oates, and Krishnamurthi (2011). They performed an experiment with 33 participants where the participants were asked to modify their privacy settings for various scenarios. They ultimately found that users wanted more fine-grained control but with fewer complicated options (p. 2300), which is consistent with some of the other studies on EHRs (Caine & Hanania, 2012; Prasad, Sorber, Stablein, Anthony, & Kotz, 2012; Weitzman, Kaci, and Mandl, 2010). Egelman and colleagues did a second

experiment, described in the same paper, in which they designed a new interface for access control within Facebook which was based on Venn diagrams. In this interface, each network was depicted as a set, where sets could overlap, and for each subset the participant could select "allow" or "deny" from a drop-down box. Changing this value caused the nested subsets to also change to the same value. Colors were also used to fill the spheres: red for deny, green for allow (p. 2301). This usability study asked participants to perform similar tasks as the previous experiment and ultimately found that participants made equal or fewer errors with the new interface. Though the SGHIx is more focused on what data to share and how, rather than who specifically it is shared with, the importance of visual aids demonstrated in this study is relevant to this project.

Madejski, Johnson, and Bellovin (2011) also examined privacy settings in Facebook. Their goal was to examine whether users' privacy settings matched their sharing intentions. They presented 65 university student participants with a table of information categories (religious, political, alcohol, work, etc.) and profile groups (friend, friend of a friend, not a friend, etc.) and asked them to fill in the table to demonstrate their sharing intentions of what they would share with whom. They then examined each participant's data using a special Facebook application to identify potential violations of their sharing intentions, then shared these violations with the participant. Each of the participants had at least one sharing violation based on their stated sharing intentions. Though their findings are specific to Facebook's privacy settings, the result that not a single participant knew exactly what they were sharing with whom demonstrates again the importance of fine-grained controls with clear descriptions. Again, this is motivation that the SGHIx

should use fine-grained access controls. This study also presented a methodology that could be useful for a future assessment of sharing within the SGHIx.

A third main area of research related to this project includes research on usability and user interface design considerations for similar systems where personal information is shared. In their article, Middleton et al. (2013) respond to concerns that EHR systems may cause unintended consequences, and even patient harm. The American Medical Informatics Association (AMIA) Board of Directors convened a Task Force on Usability to produce a set of recommendations to enhance patient safety within EHR systems, based on a thorough review of existing literature. Though much of their review focused on the use of EHRs by physicians rather than patients, the recommendations still apply to a system such as the SGHIx since similar sensitive information is shared within the system. The review uses the definition of usability from the Healthcare Information Management and Systems Society (HIMSS), "which includes nine attributes: simplicity, naturalness, consistency, forgiveness and feedback, effective use of language, efficient interactions, effective information presentation, preservation of context, and minimization of cognitive load" (p. e3). The review also takes note of 14 usability principles from the National Center for Cognitive Informatics and Decision Making in Healthcare. These principles are:

1. Consistency - Design consistency and standards utilization
2. Visibility - System state visibility
3. Match - System and world match
4. Minimalism - Minimalist design
5. Memory - Memory load minimization
6. Feedback - Informative feedback
7. Flexibility - Flexible and customizable system

8. Message - Useful error messages
9. Error - Use error prevention
10. Closure - Clear closure
11. Reversibility - Reversible actions
12. Language - User language utilization
13. Control - User control
14. Documentation - Help and documentation (p. e3)

In their recommendations, AMIA recommends that a health IT industry coalition develop a common style guide for the patient-safety functions of EHRs. They also recommend that the industry utilize usability assessments for a select set of use cases. Those two items are just recommendations at this point, they are significant to the SGHIx project and the project should follow these recommendations.

Avancha, Baxi, and Kotz (2012) compiled a survey of the literature on privacy challenges in mobile computing and communication technologies as it relates to health information technology. The most relevant topic to SGHIx is the section on Human Interfaces for Privacy Management. In designing usable privacy and security systems, Karat and colleagues identified four key issues (as cited in Avancha, Baxi, & Kotz, 2012, p. 3:31). First is that a user's main goal in using a system is to complete the task at hand and not to protect their privacy, thus controls should be transparent but also accessible. Second, the system should be accessible by users of all technical skill levels. Third, users will not use a complicated system. Fourth, the design should allow for administrative updates to comply with changes in regulatory requirements. On a similar topic, Cranor "determined that the three most important areas to users were: the type of data collected, how data would be used and whether data would be shared," as well as the finding that users "wanted the interface to be extremely simple, but they also were reluctant to have their

choices reduced to several pre-configured settings such as high, medium and low" (as cited in Avancha, Baxi, & Kotz, 2012, p. 3:32). These findings reiterate that the SGHIx system should enumerate privacy options for simplicity, but at the same time provide enough options to meet all needs. The system should also present as much detail as possible when an information consumer requests a particular data set from a user.

Though not focused on the interface design specifically, Besmer, Watson, and Lipford (2010) explored the application of social navigation to access control policy configuration. Social navigation is defined as "the use of social information to aid a user's decision," and it may aid users in selecting privacy settings by informing them of the previous decisions made by themselves or others (p. 1). They used Amazon Mechanical Turk (a system in which anyone can post a small job or task, called a HIT, to be completed in exchange for money) to recruit 390 valid participants (removed outliers based on time to compensate for participants completing the task just to earn money). Participants were asked to install a custom Facebook application, which then presented them with options for adding additional Facebook applications and privacy options, some of which included social navigation cues. Overall, they found that "social navigation does have some impact on users in the domain of access control settings for social applications, but only with a strong cue" (p. 7). Additionally, they noted that "in certain situations the participant may feel that it is easier not to authorize an application rather than configure a custom policy and uncheck a number of boxes" (p. 6). Though this study did not focus on mHealth data specifically, it raises the possibility of presenting the SGHIx users with cues when selecting their settings. The SGHIx system should assign a

default sharing setting, which may or may not be based on social navigation, but this study demonstrates the importance of selecting a default value to keep the user from feeling overwhelmed and simply opting out completely.

# 3. Use Case Descriptions

Through discussions with the SGHIx project lead, Tom Caruso, three primary use cases were identified in which the user's awareness of how their information is shared is relevant. Use cases from the information consumers' point of view were discussed, but only in terms of gathering requirements for the use cases related to the information producers. These additional use cases are outside the scope of this project. The selected use cases were developed in detail over the course of several meetings. Each use case is described in a section below.

Relevant to all three use cases are the possible options for how a user may share their data within the system. These options were enumerated and developed during the discussions with the SGHIx project lead, Tom Caruso. These options include:

- *Share my de-identified individual data* – This is the most open option. The information consumers would be able to see each data point within the set of data shared (such as Fitbit steps) but should not be able to identify the user from the data. Information such as age and gender may also be shared, but not enough information that would identify the user.

- *Share my data in aggregate form only* – This option is expected to be the most common selection. Information consumers would be able to see an aggregated collection of data from users within a range of ages, for example, but they would not be able to pick out a single user or a single user's data set from within the aggregate collection.
- *Share my data by request only* – This is a restrictive option where information consumers would have to explicitly ask to use the data set. The request would specify exactly what information would be collected and how it would be used. If a user is uncomfortable sharing their data, this option would provide more information, on a request-by-request basis, upon which they can base their decision to share their data or not.
- *Don't share any of my data* – This is the most restrictive option where no information consumer in the SGHIx system would be able to see any information about the data set.

As the SGHIx project is implemented, the options for sharing may expand based on the capabilities of the system. For example, sharing identifiable data may become an option if it doesn't violate any privacy regulations such as HIPAA. At the time of this project, the most prominent options were selected.

## 3.1 Control Access

This use case involves the user specifying who has access to how much of their data. There are two pieces to this. First, the user should be able to select a default setting which

would apply to new data as it is uploaded. Second, the user should be able to view and modify this setting for any data set at any point. In addition to being able to select the setting, the user should also understand what the setting means to be able to make the best choice and be aware of how their data may be seen from information consumers within the SGHIx.

Given the goal of ensuring that the user understands the setting, and considering the findings from prior research (Caine and Hanania, 2012; Egelman, Oates, and Krishnamurthi, 2011; Prasad, Sorber, Stablein, Anthony, & Kotz, 2012; Weitzman, Kaci, and Mandl, 2010), the options should be kept as simple as possible while still allowing for fine-grained control. This could be accomplished by presenting a finite set of options which allow the user to select a reasonable option, without presenting too many options that they are unable to choose. There is a balance between providing sufficient flexibility in the options without overwhelming the user as they select the appropriate option for their specific data.

## 3.2 Monitor Access

Once a data set has been uploaded and the control access setting has been selected, then the user should be able to view how that data has been used. Most importantly, the user should be aware of the type of data that has been shared and who has seen it. In some respect, this is a history view of the control access use case. Since users are granted rewards for sharing their data, this information should to be visible as well.

### 3.3 Accept Request

As part of access control, a user may require that their data can only be used when explicitly requested. In this case, the information consumer will provide details about the specific data desired and how it will be used. The user will then receive a request specifying these details and will need to accept or deny the request. A new request will be received each time a consumer wishes to use a particular data set. This project was focused on the interface for how a user receives the initial request from an information consumer. The user should be presented with enough information to make an informed decision about whether or not to grant access to his or her data.

## 4. Interface Designs

As part of this project, two interface design options were designed for each of the three use cases described previously. Each design presented the information in a slightly different way. The designs were then presented to the SGHIx project stakeholders for feedback. The following sections describe the initial designs, prior to any feedback. Each design is preceded by a description and each set of designs for a use case is followed by a rationale section.

Design of the home page and overall website architecture for SGHIx was outside the scope of this project. However, the designs presented here assume the existence of a personalized home page that each user would see upon logging in to the SGHIx. For

example, if might be called “My Data” and contain links to easily switch between controlling access to data, monitoring data, and viewing requests. The SGHIx project proposal (T. Caruso, personal communication, September 20, 2013) describes possibly providing data analytics and visualization tools. Again, this was outside the scope of this project, but this type of information may also appear on a “My Data” page, giving it a dashboard type of feel. Though not discussed with stakeholders, this page may roughly look something like the design shown in Figure 2 below. The secondary navigation bar could be presented as a navigation menu on the left side of the page instead. This design would require additional user research and is presented here only to provide an idea of navigation between use cases.

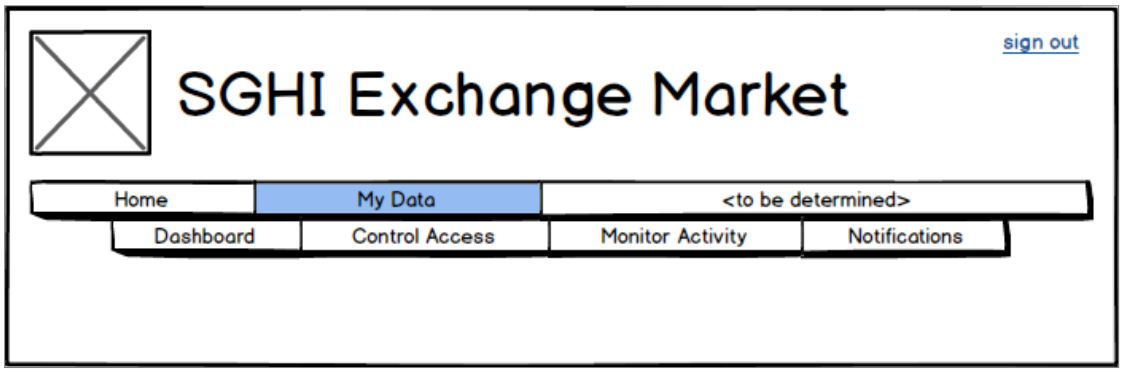


**Figure 2.** My Data page

## 4.1 Control Access

This use case was split into two main interfaces, one for an initial setting and one for existing data. Figures 3a, 3b, and 4 depict different options for how an initial sharing setting may be selected. This initial setting would likely be selected when the user first creates an account in SGHIx and it would be used as the default setting for all data

uploaded. The first design option for an initial setting is shown below in Figures 3a and 3b. These are two slightly different options of the same general design. Both enumerate the sharing setting options, as described in the use case description. The first, Figure 3a, displays one setting at a time and the slider on the left would be moved to select and display the other options. The four available levels correspond to the four options previously enumerated in the use case introductory section, also named explicitly in Figure 3b. The second, Figure 3b, displays all options at once as a set of radio buttons. A detailed description for each setting is shown as hover text. These two variations would display the same information but only vary in how much information they display at once.

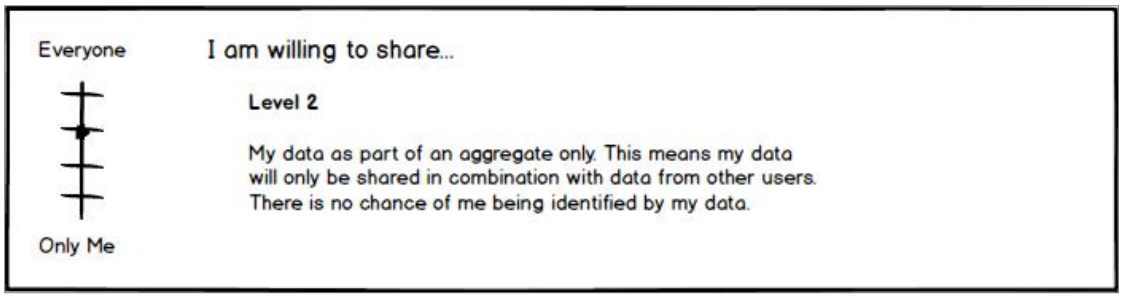


**Figure 3a.** Control Access, Initial Setting, Design #1a

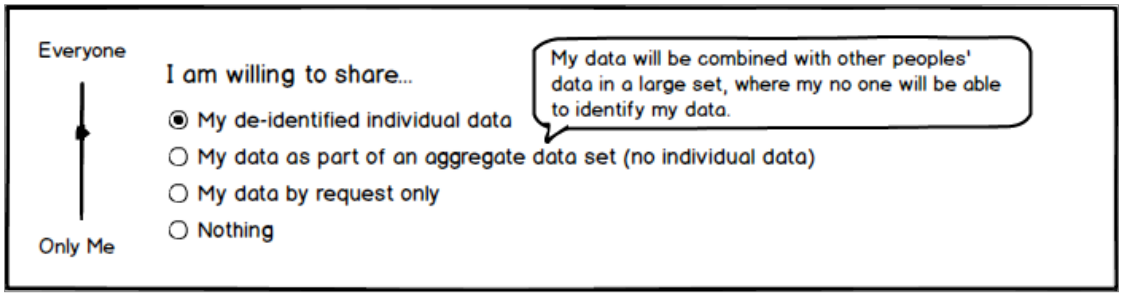


**Figure 3b.** Control Access, Initial Setting, Design #1b

The second design option for the initial setting is shown in Figure 4. This option is displayed as a table of radio buttons such that each type of data can be set to a different setting. Types of data would be pre-determined by the system according to the types of data the user has uploaded and how they fit into pre-determined categories. Primary categories may be GPS data, steps (from Fitbit, for example), and weight and food (from MyFitnessPal, for example). Alternatively, these may instead be better presented as the source of the data, such as Garmin, Fitbit, and MyFitnessPal, for example. The sharing setting options are displayed in the column headers and are the same as those in the first design option. As with the previous design option, a detailed description of each setting would be displayed through hover text.

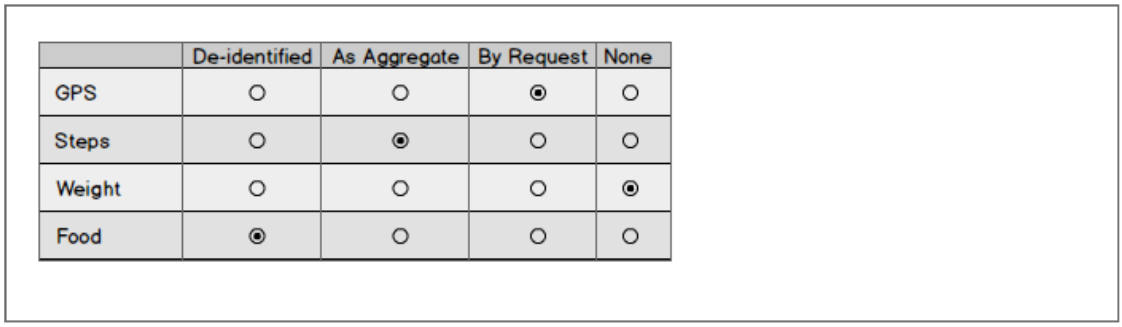


**Figure 4.** Control Access, Initial Setting, Design #2

A user may not wish for the same setting to apply to all of their data, so they should be able to change the setting for each existing data set. This is depicted in Figure 5, presented as the interface to modify access to existing data. In this design, each existing data set is listed with an appropriate icon next to it. Then a drop down list of possible sharing settings is displayed. The setting is greyed out to indicate it has been set. Clicking

the edit icon next to the setting will enable the drop down box such that the setting can be changed. Rather than using hover text for a detailed description of each setting, this would be displayed below the list of current settings. As compared to the initial setting option presented in Figure 4, the data sets displayed in Figure 5 are different. The reason for this difference was to trigger conversation in the review with stakeholders as to which is the better way to present the sets of data.

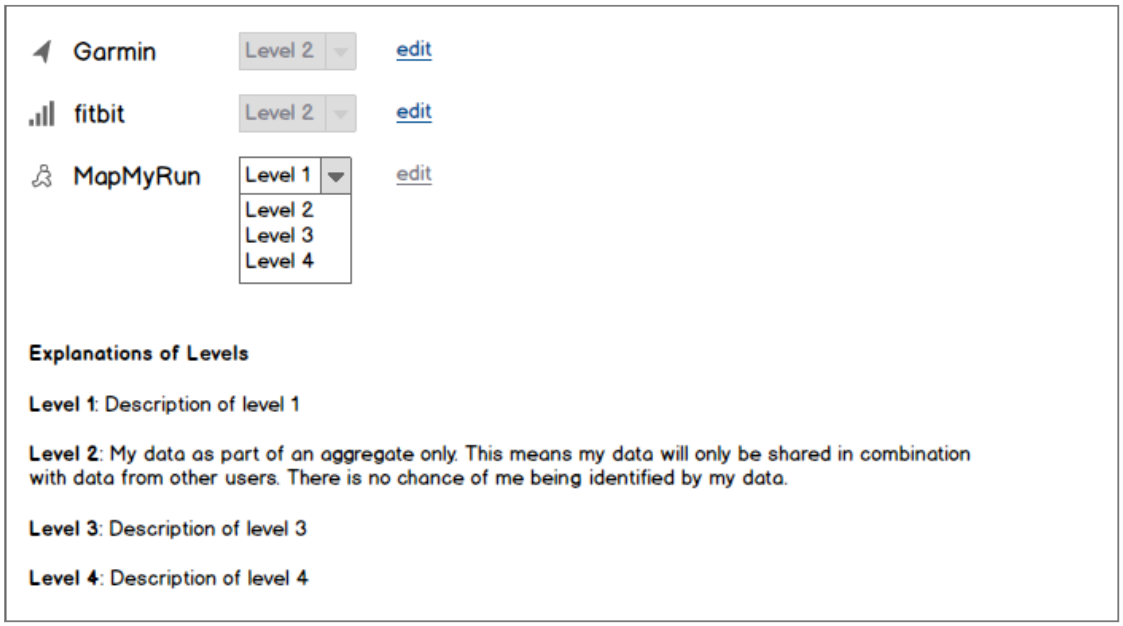


**Figure 5.** Control Access, Existing Data

## Rationale

For Design #1, shown in Figures 3a and 3b, the idea was enumerate the possible options for how data may be shared. A slider was included to indicate that the options lie on a scale between everyone or no one being able to see the data. Inspiration for this design came from the Internet Explorer's Security setting, shown in Figure 6 below. This was

chosen because it provides a limited set of choices yet covers all of the available options. Design #2 for the initial setting, shown in Figure 4, took into consideration that a user may wish for this setting to be different for different types of data. For example, some people may feel that GPS data is more private since it could potentially indicate where they live. The inspiration for this design came from Fitbit's Privacy Settings interface, shown in Figure 7 below. Once again, this is a clean way to present many options without overwhelming the user with too many choices. Design #2 shows significantly more options and may ultimately be too much detail for users in the initial default setting screen.

Another design consideration to add awareness to the different levels of data sharing would have been to add color, such as a green to red scale. However, since the purpose of the SGHIx is to share data, displaying something in red may discourage the user from selecting the setting. Though one setting may be a higher privacy risk than the others, that does not mean that the user should not select it.

For modifying the setting on existing data, Figure 5 shows one possible option. In this option, each type of data appears in a list with its current setting next to it. This design shows the settings labeled as numbered levels, but ideally these levels would be standardized such that a more descriptive name could be used and the user would not have to look up what Level 2 means, for example. The levels are those described in the use case description section, where they are identified by a longer name. The other designs present these levels with descriptive names, but a usability evaluation or a survey

of potential users could reveal the best names to use. As with color, numbered levels may inadvertently discourage users from sharing their data. For each type of data, the user could edit the setting and select a different option from the drop down menu. A second option for modifying existing settings, which is not explicitly presented here, would be the same table of radio buttons as shown in the initial setting Design #2 in Figure 4. This option would make it easier to glimpse at the screen and see which data sets are set to a higher or lower sharing setting. One tradeoff is that it would not have the edit links as shown in the design in Figure 5, meaning it may be more difficult for a user to know when they have made a change to their settings. Ultimately, the preference between the two designs could depend on the amount of varying data types a single user shares as well as how often the users review and modify their settings.

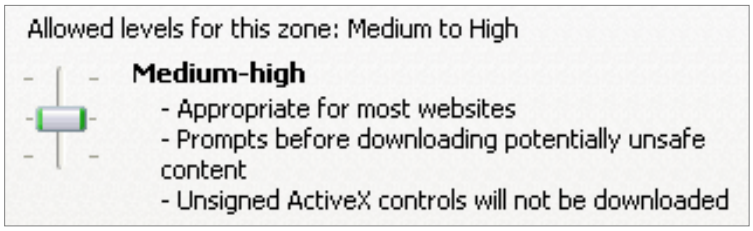


**Figure 6.** Internet Explorer Security Setting

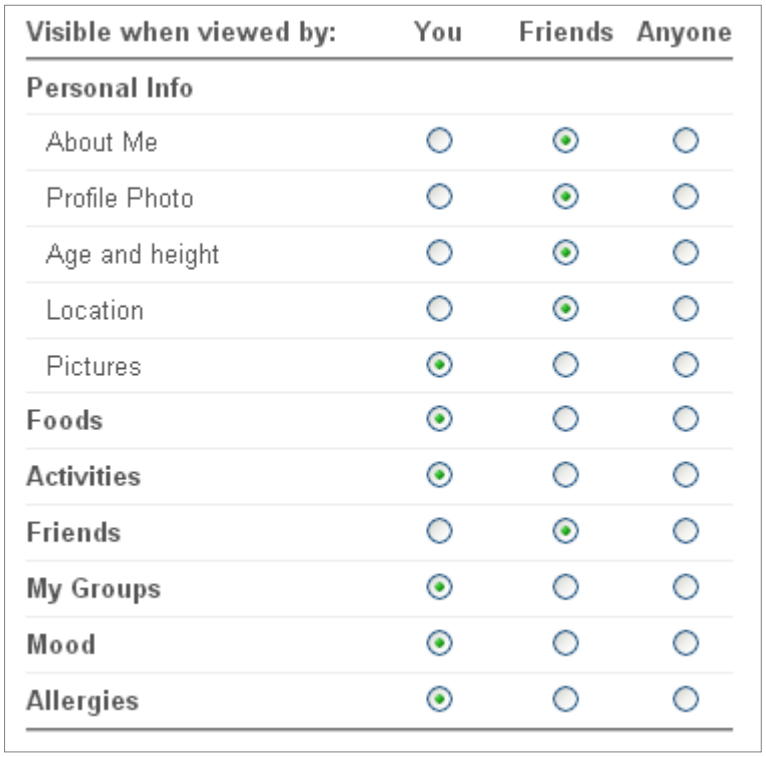


**Figure 7.** Subset of Fitbit Privacy Settings

## 4.2 Monitor Access

The first design option for the Monitor Access interface, shown in Figure 8, displays each data set in collapsible sections, such that only one section is expanded at a time. The header bar for each section contains an icon for the data, the source of the data, how recently it has been used by an information consumer, and the number of points acquired from sharing the data. The points may ultimately be some other form of reward, but for this design points were selected to indicate the value of the reward. Within each section is a table containing details on which consumers have used the data, what date the information was used, and details about how the data was used. If additional information is available, it could be presented as hover text over the applicable row in the table. This

view provides the user with feedback on how frequently and in what manner their data is being used.

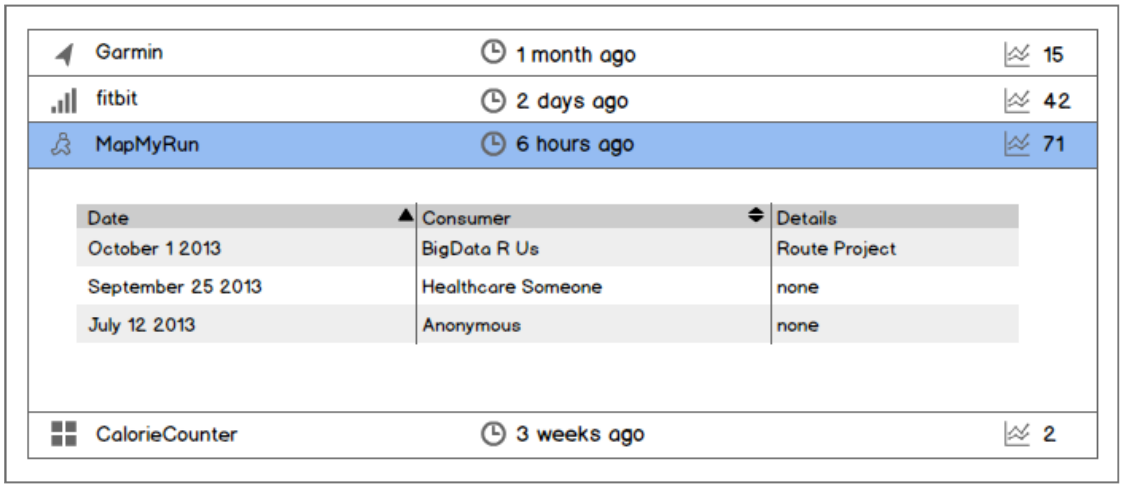


**Figure 8.** Monitor Access, Design #1

The second design option for monitoring access, shown in Figure 9, instead displays the same type of information in one big table. This table can be filtered by any values for any of the columns and it can also be sorted by clicking on column headings. All values present for any column in the unfiltered table would be available as options to filter that particular column on. For example, a user may want to see all data use by a particular consumer, or only within a particular time span, or even both. Filters can be used in any combination. The column for explicit request indicates occasions when an information consumer sent a request for data rather than using it in aggregate form. For example, users may require requests for GPS data but allow Fitbit data used in aggregate. This would mean that the table would indicate explicit requests were made for the GPS data source but not for the Fitbit data source. However, since a user can change these settings

at any time, GPS data, for example, may not always be consumed only by explicit request. As with the previous design option in Figure 8, additional information for any particular row would be displayed as hover text when available.

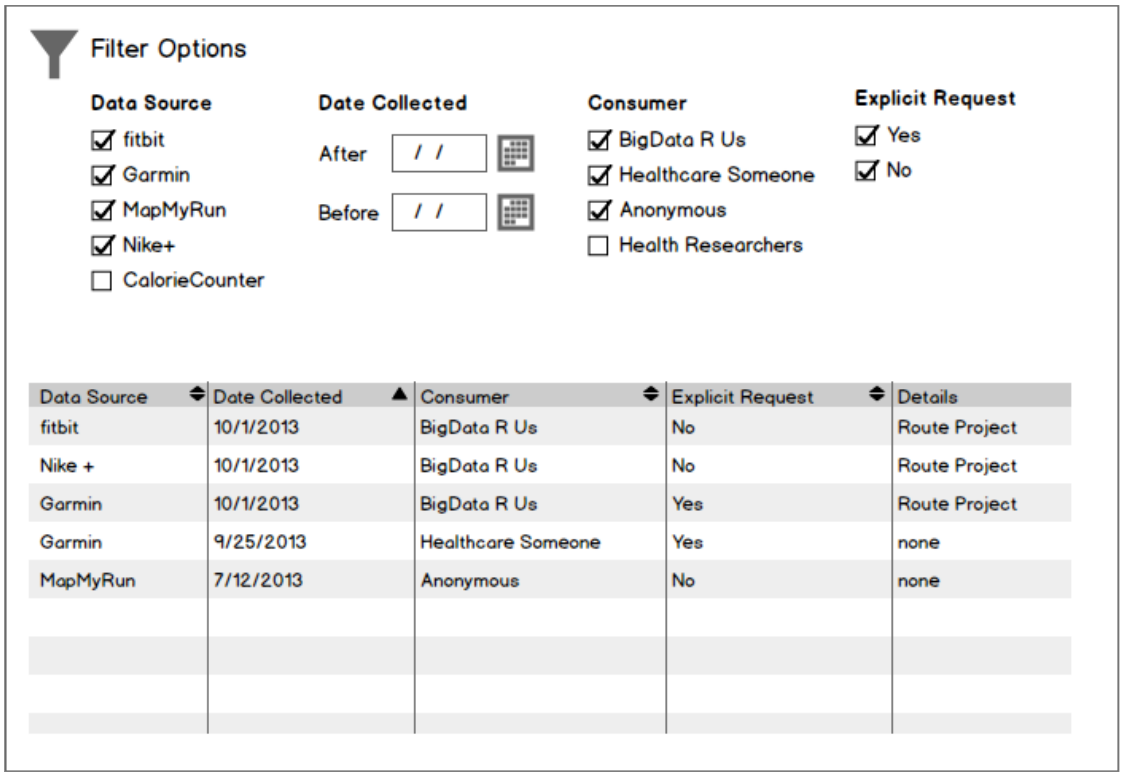


**Figure 9.** Monitor Access, Design #2

**Rationale**

For this use case, the primary goal is for the user to be able to easily check to see if and how their data is being used. One design consideration was the difference between a push or a pull model. In some cases, for the most sensitive data, a user may wish to be notified by a push notification when their data is used. Though a push notification may be an

option in the future, this project focused on the pull model, where the user must go to a specific page in order to view the information.

Design #1, shown in Figure 8, uses an accordion style container element of collapsible sections. This container was selected because it allows the user to see information about one particular data set at a time, which helps to keep the user from being overwhelmed with too much information at once. Design #2, shown in Figure 9, includes the same type of information, but in one large sortable and filterable table. The reason for using a large table is that a user may wish to see certain information across data sets, rather than being restricted to one data set at a time. For example, a user may wish to see data used by a particular consumer, or data used within the last month. Rather than displaying data by the name of the data source, it could alternatively be displayed by type of data, such as GPS, steps, etc. Though not listed in the design, reward points should also be included as a column in the table and a user may wish to which data sets have earned them the most points. Preference between these two designs may ultimately depend on how much data one user uploads and how often that data is viewed. Predicting these quantities is outside the scope of this project, but the two design options should support both large and small amounts of data.

## 4.3 Accept Request

The first design option for accepting requests from information consumers is shown in Figure 10. In this design, a single table is used to show all incoming requests. The table contains columns for the name of the requestor (or consumer), type of data, date the

request was received, and details about the request. The leftmost column contains checkboxes such that multiple requests can be approved or denied at the same time.

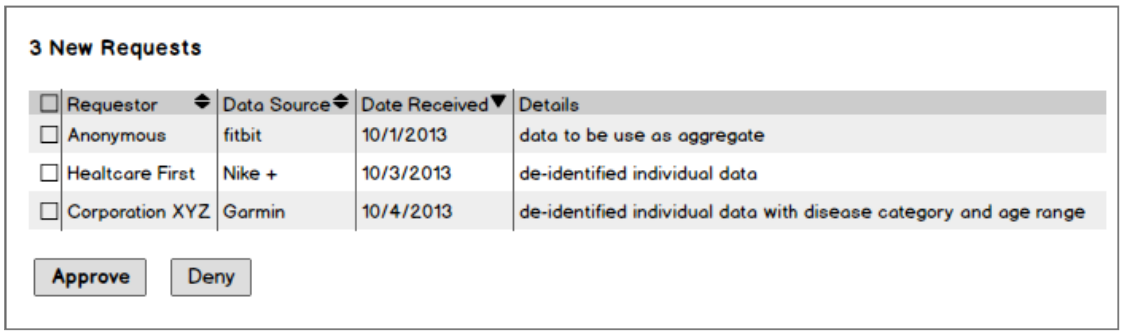


**Figure 10.** Accept Request, Design #1

The second design option for accepting requests, shown in Figure 11, lists each incoming request in its own labeled fieldset. The fieldset draws a frame around the request and includes a name at the top, such as Request 1. Each request lists all available details and can be approved or denied individually using buttons within each fieldset. The details in the example include the same details listed in the table for the first design option. However, the information consumer making the request may provide much more information and all of that available information would be displayed.

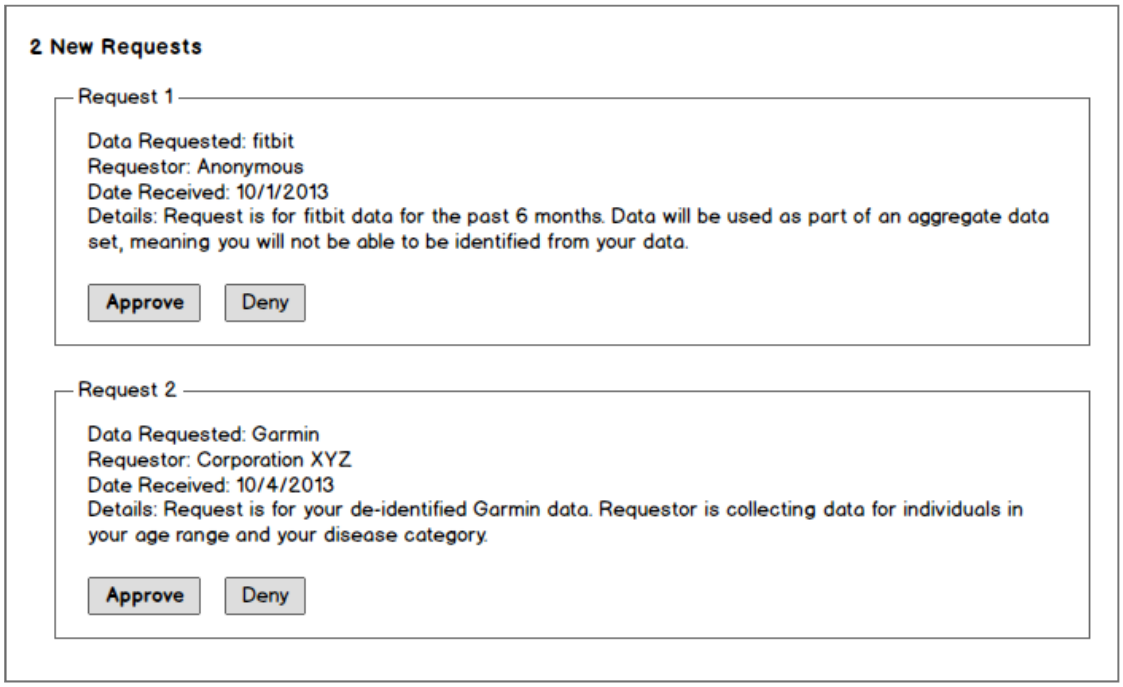


**Figure 11.** Accept Request, Design #2

## Rationale

For this use case, it is important for the user to be able to see enough information about the request to make an informed decision about whether to approve or deny the request. Design #1, shown in Figure 10, is a table of all incoming requests with details within the table. There may also be a need to have the table expand or show hover text to show additional details about a request. In this design, the user may approve or deny multiple requests at one time. This would be useful if the user receives a high number of requests. Design #2, shown in Figure 11, lists each request separately and each must be approved or denied individually. The benefit to this design is that it makes it easier for the user to read the details about the request. Ultimately the decision between these two designs may depend on the number of requests a user may receive. Given the goal of awareness, the

second design provides the most visible details for each request and may be the best for ensuring the user truly understands what is being asked in the request.

## 5. Review with Stakeholders

A meeting was held with the SGHIx stakeholders to review the interface designs presented above, with the goal of gathering feedback to be used to revise the designs. The stakeholders include about fifteen people who have been involved with the project since the beginning. The SGHIx project plans to make use of some existing software systems to download and store the SGHI data. Representatives from these organizations are included in the stakeholders groups, in addition to key members of the joint organizations that have proposed the project. Several students and faculty are also involved in the project and were invited to the review meeting.

The meeting was held on October 24, 2013 from 2 to 3 pm. A screen sharing web conference was used along with a telephone conference. Five people were able to attend in person and an additional four or five people joined online. The goals of the project were defined and then each interface design was presented and discussed.

The discussion was continuous and constructive. One key issue discussed was how to define the data sets. The original interface designs list the data by the source of the data, such as Fitbit or Garmin. However, many of the stakeholders stated that they would

rather see the data separated by type, such as steps or GPS. Part of the reason for this is that users may have multiple devices that collect the same type of data and they may wish to compare the two. The stakeholders found it more valuable to see all of your data about steps together, given that you may want to make comparisons between devices, or even perform some analysis to normalize the data. This is an item for future work, to determine how users prefer to break down the sets of information and if they perceive the data in the same way as the stakeholders. Based on the discussion, I chose to redefine a data set as the combination of a source and a type, such as Fitbit steps or Fitbit weight. Several other items were discussed in the meeting and listed below.

Topics discussed included:

- Whether data sets should be grouped by the source of the data or the type of the data (discussed above). It was suggested to let the user choose how they wish to see their data grouped.
- Whether sharing with everyone should be an option for the control access use case. Currently the most open option is to share de-identified individual data, but perhaps some users may be willing to share identified data. This is an item for future work given that allowing access to identified data raises additional privacy and security concerns not covered thoroughly in this project.
- The control access options should be clearly presented at signup vs. modifying access. Modifying access should be presented in extreme detail but the initial default setting should be as simple as possible, so as not to overwhelm the user

when they are signing up. The interfaces for these settings could also remind the user that they are signing up with the system in order to share their data.

- The radio button option for controlling existing access was preferred to the option with dropdown boxes for the setting.
- Icons should be used when possible since the interfaces are too text based. An example was sketched on the board to show the different levels of sharing. An icon of a globe could indicate sharing with the most people while a small set of people within a box would indicate sharing with a set of people. Then an icon of individual people would indicate the most restricted sharing where only specific people can see the data. The use of a diagram to show who can see what, such as a Venn diagram, was also mentioned but not sketched out.
- It may be possible to de-identify GPS data such that points are relative to each other rather than latitude and longitude coordinates. This could make GPS data less sensitive but is outside the scope of this project and is instead an item for future work.
- Units, such as steps, miles, calories, heart rate, etc. may need to be considered. This may be one way that data could be grouped together.
- Several stakeholders were concerned with maintaining simplicity for the first prototype of the SGHIx system. The rollout of the system is outside the scope of this project, but the preference to start with a minimal design and include only the most critical options was noted. Stakeholders also expressed a desire to request feedback from the initial users of the system, which is also outside the scope of this project. A formative usability is an item for future work.

- When a request is made it should specify as much as possible about how the data will be used. Given that explicit requests will likely only be made for the most sensitive types of data, the user will want to know as much detail as possible to determine whether to accept or deny the request.
- Somewhere within the system it may need to be noted that the benefit a user receives for sharing data may depend on the quality of that data. Again, this is outside the scope of this project but helpful for understanding how the reward system may work and may influence how that information is presented.
- It was suggested that de-identified data could be downloaded by the information consumers with access to that data, but data used in aggregate form may be only viewable and not downloadable. This distinction could be important because if an information consumer has downloaded your data, and then you change your sharing setting for that data to restrict sharing, there is no way for the system to take that data away from the information consumer who has downloaded it. This distinction is not finalized and is thus not made evident in the interface designs. However, it should be considered for future versions of the interfaces.

# 6. Revised Interface Designs

Based on the review with the stakeholders, the interface designs were revised and are presented below. For each use case the revised interface designs are preceded by a discussion about the decisions and revisions made.

## 6.1 Control Access

During the meeting with stakeholders, it was clear that the initial setting should be as simple as possible, while still providing all the information necessary to ensure the user is aware of the implications of the selected setting. One of the stakeholders expressed concern that a complicated sign up process may deter new users. Though designing the complete signup process was outside the scope of this project, this desire for simplicity was taken into consideration. Since the initial setting for controlling access would be during signup, Figure 12 shows a simplified version. The setting that data can be used as part of an aggregate data set enables the sharing of SGHI within SGHIx, without limiting the sharing too much. Also, it was highlighted in the review meeting that users who create an account within SGHIx do so with some existing desire to share their data, since that is the purpose of the system. Therefore this setting was selected as the default, such that new users can read a short paragraph about the setting and then continue on. The user does not have to make a decision on which setting to use, but rather to keep or modify the default setting. An icon was also added to indicate use in an aggregate, improving the user's understanding of how the data would be used.

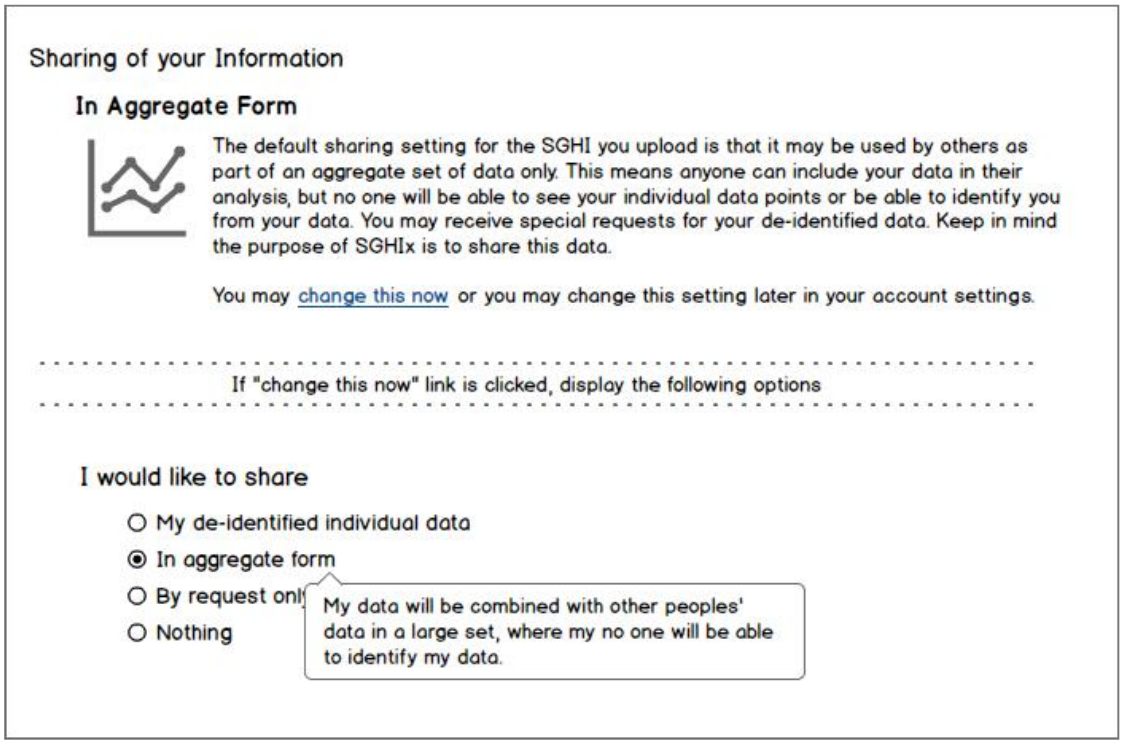


**Figure 12**. Control Access, Initial Setting, Redesigned

The redesigned interface for modifying existing access controls is shown in Figure 13 below. A design decision was made to present the access control options as a table of radio buttons in order to give users an always-visible, always-changeable view of the options. In this redesign, the variable ways to break down the data sets were modified so that the user can select how they wish to view the settings. They may view the table by data source (such as Fitbit, Garmin), data type (such as steps, GPS), or ungrouped, meaning each combination of data source to data type would be shown as a separate row (Fitbit steps, Fitbit weight, Garmin GPS, etc.). Another feature of the redesign is the addition of icons, which could be customized to the specific icons of the data source. The icons selected for the sharing setting should be standardized and used throughout SGHIx. Icons could also be placed inside the rows of the table rather than to the left side. In the

redesign, the icons represent a key term in the setting, such as individual, aggregate, request, or none. Another option for the icons may be to use some that are comparable to each other, such they could indicate a scale of settings. For example, a globe may be used to indicate complete visibility along with sets of people to indicate individual data or as an aggregate.

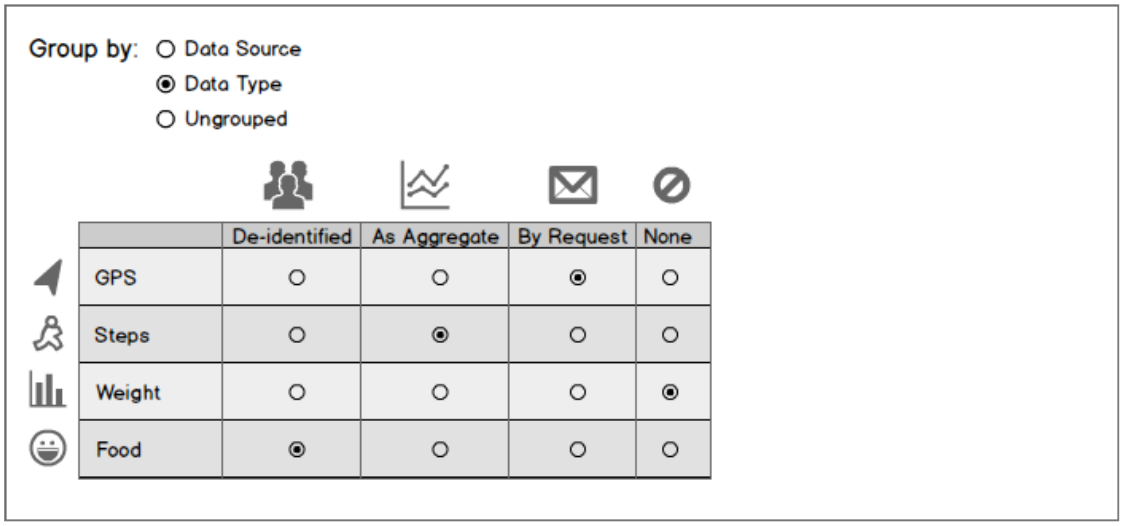


**Figure 13.** Control Access, Existing Data, Redesigned

## 6.2 Monitor Access

The primary change in the redesign of the interface for monitoring access, shown in Figure 14, is related to the grouping and presentation of the data sets. Rather than grouping data by source or type, the combination of the two is used for each data set. This decision was made because it presents the data in the smallest sets. If work is done in the future to determine how users wish to view their data, then the small data sets could be grouped by source or type instead. The ability to allow the user to decide how to

group the data added a level of unnecessary complexity to the interface, thus the small data sets were determined to be a simpler presentation. An information icon was added next to the name of each consumer. This icon would be used to provide additional information about how the data was used, when available. Most likely the information would be presented as an overlay when hovering over the icon and may include a link a page with more details. It should also be noted that the user should be able to easily get to the control settings pages from this page. Using the sample navigation bar presented previously in Figure 2, the ability to easily get from monitoring access to controlling access is a key piece to ensuring the user is aware and in control of how their data is consumed.

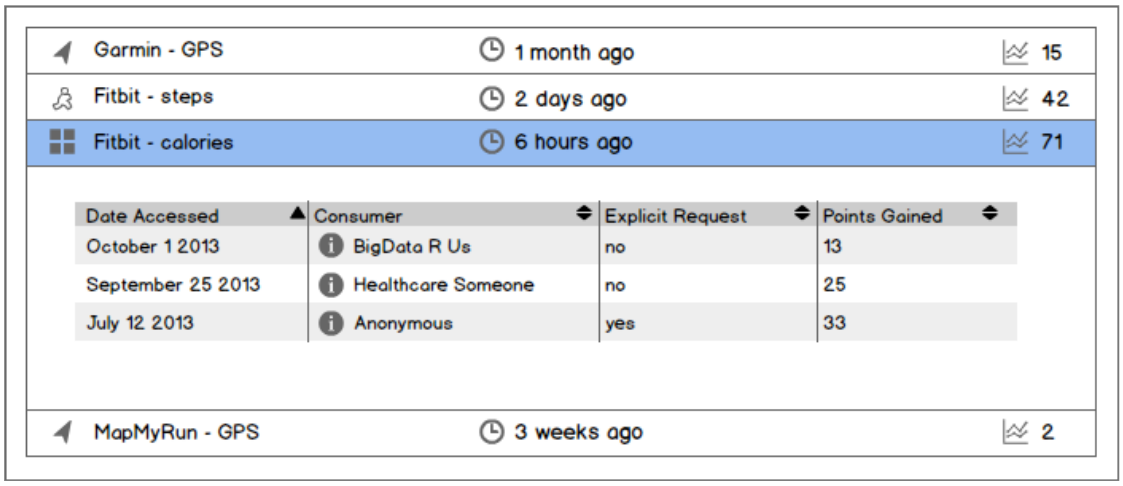


**Figure 14.** Monitor Access, Redesigned

## 6.3 Accept Request

The stakeholders agreed that users would typically only require explicit requests for their most sensitive data types. Most examples presented in this project are for step or GPS

data, but SGHIx will be able to handle all sorts of data, possibly even data that a user may only wish to share with his or her doctor. An example of this sensitive data may be related to a disease or blood pressure condition.

Given that the requests will primarily be for sensitive data, the redesign shown in Figure 15 displays only one request at a time. This is so that as much detail as available can be shown about the request and the consumers intended use of the data. When possible, an icon will be shown to represent the type of data requested. Additional icons could be used to represent the information that would be tied to the data, such as age and gender. In requests for more sensitive data, this additional information may include disease category or zip code. For each request, the user can approve, deny, or ignore the request. Clicking any of those buttons would then display the next request if there are more pending.

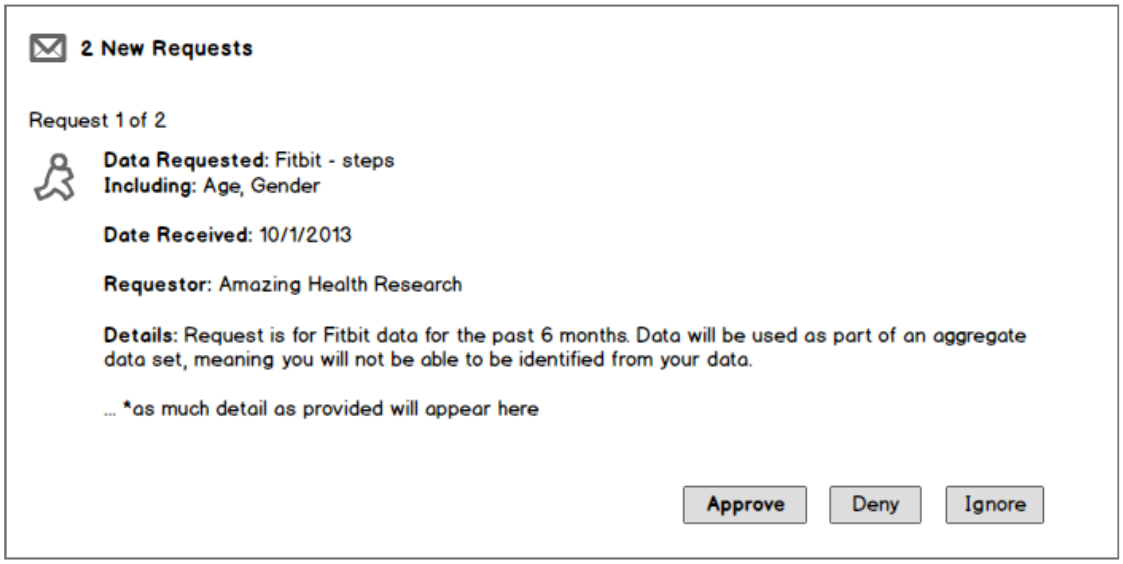


**Figure 15.** Accept Request, Redesigned

# 7. Conclusion

The interface designs presented in this paper show how a SGHIx system could be implemented to support users' sharing their SGHI data while also supporting their needs to remain aware of who is using their data and how. The review session with stakeholders provided productive feedback which was incorporated into the revised designs.

# 8. Future Work

Since the SGHIx project is still in the planning and early development stages, it would be a great candidate for user-centered design studies. The designs presented in this paper could be prototyped and then tested in a formative usability evaluation. Specifically, grouping data sets by source or type of data should be evaluated. The wording of the descriptions of the sharing settings should also be evaluated to ensure that they are clear. Also, the option to require explicit requests may need to be separate from the list of sharing settings. This project included it as one of several options, but users may prefer to select a default setting and then independently specify if they would like to receive requests to share more detailed data. This could be examined in a usability study as well. Such a usability study should be done with users and their own data, to ensure that the results are the most reliable and predictive of future users of the system (Prasad, Sorber, Stablein, Anthony, & Kotz, 2012).

As a compliment to a usability study, the project could benefit from a of survey sent to potential users to answer questions about the data they may be willing to share and the type of reward that should be offered for sharing SGHI. Though a survey could only discuss hypothetical data and can't put users in the position of actually sharing their data, much information could still be gathered from a survey. This information could help solidify some design aspects of the overall SGHIx system, such as the specific sharing options that should be enumerated and the preference for how data sets should be grouped, and thus influence the interfaces designed in this project.

The review meeting with stakeholders raised several questions for future work, including whether data could be shared with everyone. This may depend on what restrictions the system has with respect to privacy regulations such as HIPAA, but additional investigation is required. It was questioned if GPS data can be (and should be) de-identified. This ability may encourage users to share even more data, and thus the possibility of de-identifying this type of data should be pursued. Finally, once the system architecture is determined, any clarifications on what type of data, if any, an information consumer can download should be determined. If consumers are given the option to download any data, this needs to be clearly presented to the user.

**Bibliography**

Avancha, S., Baxi, A., & Kotz, D. (2012). Privacy in mobile technology for personal healthcare. *ACM Computing Surveys (CSUR), 45*(1), 3.

Besmer, A., Watson, J., & Lipford, H. R. (2010, July). The impact of social navigation on privacy policy configuration. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (p. 7). ACM.

Caine, K., & Hanania, R. (2013). Patients want granular privacy control over health information in electronic medical records. *Journal of the American Medical Informatics Association, 20*(1), 7-15.

Caruso, Tom (2013). *SGHI Exchange Market*. Retrieved from http://www.sghiexchange.org/

Egelman, S., Oates, A., & Krishnamurthi, S. (2011, May). Oops, I did it again: Mitigating repeated access control errors on Facebook. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2295-2304.

Li, J. (2013). Privacy policies for health social networking sites. *Journal of the American Medical Informatics Association, 20*(4), 704-707.

Madejski, M., Johnson, M. L., & Bellovin, S. M. (2011). The failure of online social network privacy settings.

Middleton, B., Bloomrosen, M., Dente, M. A., Hashmat, B., Koppel, R., Overhage, J. M., ... & Zhang, J. (2013). Enhancing patient safety and quality of care by improving the usability of electronic health record systems: recommendations from AMIA. *Journal of the American Medical Informatics Association, 20*(e1), e2-e8.

Prasad, A., Sorber, J., Stablein, T., Anthony, D., & Kotz, D. (2012, October). Understanding sharing preferences and behavior for mHealth devices. *Proceedings of the 2012 ACM workshop on Privacy in the electronic society*, 117-128.

Weitzman, E. R., Kaci, L., & Mandl, K. D. (2010). Sharing medical data for health research: the early personal health record experience. *Journal of Medical Internet Research, 12*(2).

Yasnoff, W. A., Sweeney, L., & Shortliffe, E. H. (2013). Putting Health IT on the Path to Success. *JAMA, 309*(10), 989-990.