Exploring Consent and Authorization Voice Interface for Healthcare Privacy

Chenxiao Guan (chenxiag@andrew.cmu.edu)
Chenghao Ye (chenghay@andrew.cmu.edu)
Yigeng Wang (yigengw@andrew.cmu.edu)
Fangxian Mi (fangxiam@andrew.cmu.edu)

18, Nov, 2020

Abstract

People are accustomed to letting voice assistants complete daily tasks for more convenience, and the purpose of our design is to provide healthcare services to people via voice assistants as well. However, news and studies show many devices have been exposed to record and abuse users' conversations with intelligent voice assistants without consent. Thus, we created a consent and authorization voice interface using Alexa Skill based on HIPAA Privacy Rule to guarantee users can handle their protected health information (PHI). We innovated a new way of agreeing to privacy policies and notices via a voice interface, while still maintaining the usability from the user's perspective in a privacy-friendly manner, and simultaneously letting the company-side be in compliance with regulations such as HIPAA. The implementation is meant to strike a balance between usability and privacy-friendliness, and thus we provide a way of configuring fine-grained privacy preferences while making sure the interface is not bloated with too many explanations that annoy our users. Users are able to use the skill for general purposes without providing their credentials to their health records. What's more, they can also access and configure privacy preferences within the skill after linking their accounts. To examine the effectiveness of our sample skill, we conducted semi-structured interviews with 12 participants to obtain the feedback on our consent and authorization interface. In the end, we present a set of future potential improvements to the current implementation and methodology of conducting user studies.

1. Introduction

With the advent of 5G and the widespread adoption of voice assistant technologies such as Amazon Alexa, Google Assistant and Apple Siri, it is changing the way people live while post challenges for the developers and the companies to make sure their technology is compliant with various regulations across different countries. For the healthcare industry specifically in the US, the Health Insurance Portability and Accountability Act (HIPAA) is the most important regulation that health care providers have to follow when they are dealing with protected health information (PHI) of their customers.

Although HIPAA has been enforced in the US more than a decade already, it is still unclear as how exactly compliances are made in cases where individuals are interacting with newer technologies such as voice assistants, and companies are struggling to keep making sure their products can strike a balance between usability their users standpoint, versus the miscellanies that their users have to go through before they are able to use the products, such as agreeing to the privacy policies. Although it is fairly easy to let users agree to privacy policies through a graphical interface, such as displaying a pop-up window through browser, or sending a push notification to users' mobile phone, doing it through the voice interactive interface remains a challenging field for both the technology industry as a whole as well as privacy researchers.

In order to present the viability of being able to develop an interface that is easy to use on the customer's side to agree to privacy policies so that users feel their privacy are taken care of, and also providing users the tools to configure their privacy preferences through voice interface as well, we have developed an Amazon Alexa skill that answers users questions based on their privacy settings - but most importantly, we present a straightforward interactive interface for users to agree to the privacy settings and consents while using the skill. We teamed up with Highmark Health, which is a non-profit healthcare company based in Pittsburgh Pennsylvania to conduct the research, and together we have developed the skill with all the considerations above in mind.

Throughout this research paper, we will present some of the related works in part 2, such as consent interfaces for HIPAA, voice assistants privacy concerns, etc. Then, we documented the methodology in part 3 including how the Amazon Alexa skill was implemented, what are some of the design considerations we took into account while developing the privacy consent interactive session, the actual workflow itself, etc. Since we conducted a user study with 12 participants, we have included the through process of designing the interviews, conducting them, and finally we show the results of our interview in part 4. In the end, the discussion section presents some of the key takeaways that we got throughout conducting the user study as well as developing the Alexa skill, and some limitations for the study.

2. Related work

2.1 Consent methods for Health Insurance Portability and Accountability Act (HIPAA)

Since the Health Insurance Portability and Accountability Act came out back in 1996, research and industry have tried various ways to keep themselves in compliance with the regulation, either as a covered entity (CE) or business associate (BA). Various frameworks and recommendations have been proposed and every solution has their pros and cons. This section briefly discusses some of the solutions and compares their strengths and weaknesses.

Littenburg et al. [1] proposed a passive way of letting patients allow the physicians to collect and further use their health record and personal health information (PHI) without explicitly allowing them to do that. The authors employed a way where patients are notified via physical mail that they are going to participate in a study hosted by The Vermont Diabetes Information System (VDIS), and patients are informed to explicitly opt-out the study by either calling the physician or a toll-free phone number. The proposal was reviewed by a number of IRBs as well as attorneys, other hospital's laboratories, and state-wide peer review organizations, and all of them approved that the existence of the letter was sufficient to keep the study HIPAA compliant. As a result, among the 7,558 randomly-chosen participants, only 210 (2.8%) of them chose to explicitly opt-out of the study.

Besides HIPAA specifically, researchers have been focusing on developing frameworks for making IoT consent interfaces easy to use for both data subjects and data controllers. Cunche et al.[2] proposed a generalized framework for managing consents of IoT devices, following the guidelines of GDPR and WP29. The authors follow a "declare" and "collect" methodology via either direct or indirect communications or personnel custodians, and they discuss several technologies that are possible to be used in order to achieve these types of communications between IoT devices. This could potentially be a direction for us to look into as the paper discussed the possibility of making consents beforehand via other applications and sharing the consent via the internet.

In the context of voice assistants and IoT devices, there are still ways implemented for developers or covered entities to make their applications compliant to HIPAA. As far as this paper is concerned, Amazon Alexa is now HIPAA compliant as long as the developer follows a series of guidelines provided by the official documentations[3]. The limitations needed, as compared to regular Alexa skills that do not require HIPAA compliance, are for example limited usage of the API, the requirement of agreeing to Alexa's Business Associate Agreement, usage of account linking, etc.

2.2 Privacy concerns regarding voice assistants

The purpose of our design is to provide healthcare services to people via voice assistants. Based on this situation, we conducted research on people’s privacy concerns towards smart speakers and voice assistants, for us to start a hands-on user study and research. Josephine et al. conducted diary studies and semi-structured interviews with smart speaker users and non-users to understand the motivation and unwillingness to actively use smart speakers. The results [4] show that the main reasons why most people do not use smart speakers are poor practicality or distrust of the company, and not many people have expressed concerns about privacy. This is mainly due to the complex relationship between the user and the company and the user's low level of awareness of privacy. It also concludes that convenience and identity are mainly the reasons why users use smart speakers, and usability and privacy and safety awareness are the reasons for excluding smart speakers.

In investigating the privacy attitude of users towards smart speakers, Nathan et al. [5] developed and applied a browser plug-in to record the real situation of user interaction with the device. By participating in a well-designed Survey Flow, the analysis results show that more than half of the participants did not know that their data would be permanently saved, nor did they know that they could view their past voice records. The survey results also show that users are generally worried and dissatisfied with the retention policy of smart speakers.

Anonymous authors measured the trustworthiness of Amazon Alexa in a study. The skill must be certified for content functionality and compliance with privacy-related laws before third parties can develop and release new skills. The researchers focused on skills that are certified but still violate privacy policies, and they identified 234 such skills. Among them are skills that violate HIPAA's ability to collect user health-related data. For example, the user's physical and mental health, recent medical visits, prescription drugs and so on were collected, but no consent interface was set up [6]. It explains why people have privacy issues with voice assistants, voice assistants need to be more regulated in reviewing privacy policies of certified skills.

2.3 Amazon Alexa

According to Erika and Kim [7], Alexa provides a cloud-based conversational service representing Amazon. Amazon designed the Alexa Voice Service (AVS) to simulate real conversations, at the same time, to obtain the service, users are able to actually use intuitive voice commands. In order to convert audio into text, Alexa will analyze the characteristics of the user's voice, such as frequency and pitch, to provide feature values. Given the input features and model, the decoder will determine what the most likely word sequence is [8].

From developers perspective, AVS allows developers to create “on-device software”, which is known as Alexa skill, to process the audio input from the customers [9]. What’s more, developers can also take advantage of Amazon Alexa APIs to build and manage the connections and interactions between their devices and Alexa. According to Amazon’s Developer site, these interactions are included but not limited to “speech recognition, audio playback, volume control, and hardware control” [9].

3. Methodology

3.1 Alexa skill development

We designed and developed an Amazon Alexa skill with a voice consent and authorization interface. We chose Alexa as our development platform because Alexa offers a skill market for its end users where users can enable third-party developed functionalities. This means that Amazon Alexa is very open to third-parties, which makes our development and deployment process easier. We developed the skill using the Alexa Skills Kit SDK for Node.js, and deployed our implementation using AWS Lambda. For authentication, we used AWS Cognito as our OAuth2 identity provider for mocking the actual implementation of Highmark Health's backend authentication server. Note that an OAuth2 server was required solely because in order to use the Account Linking functionality of Alexa skill, Amazon requires skill developers to use an actual OAuth server.

Based on our voice work flow, our consent and authorization interface is able to offer two specific policies for users via voice provided by Highmark Health, which are the Digital Privacy Policy [10] and the HIPAA Authorization [11]. What’s more, our Amazon Alexa skill can also provide two different services for users with or without account linking. Users can also configure their personal permission settings after linking accounts and are able to revoke their settings at any time.

3.1.1 Consent and Authorization interface

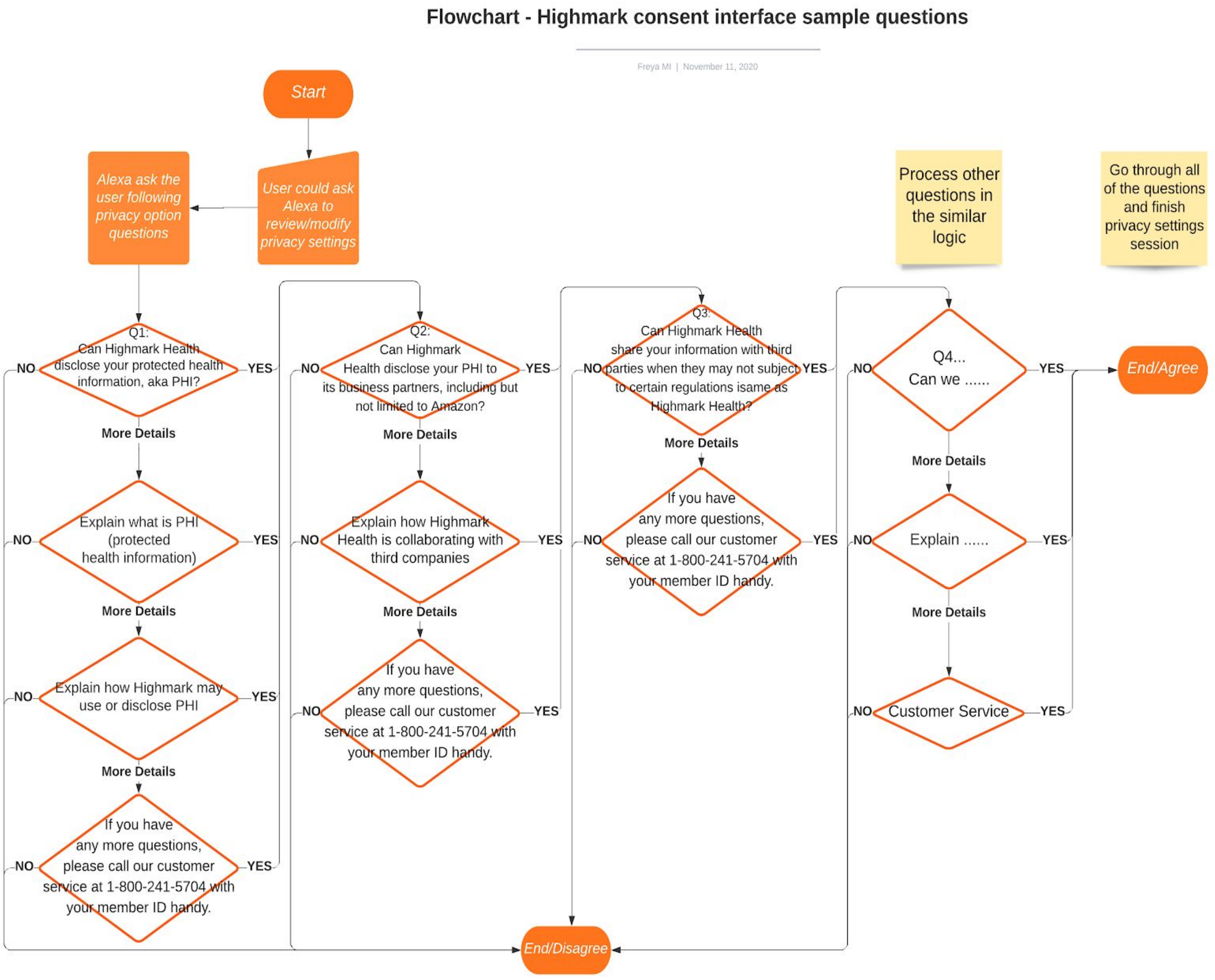
Users can access the different privacy policy via two ways through our consent and authorization interface. The first one is the traditional way, in which users can choose to read the written policies through their mobile Alexa app. What’s more, users can also listen to the privacy policy via the voice assistant.

Following the two policies and the questions workflow charts mentioned below, we implemented our consent and authorization interface. We built a graph-based question map to record the different policy question states. For each question state, it contains two children states which represent the next question and the details of the current question. This design allows the user to say “yes” to listen to the next question at any time instead of going through all the details.

3.1.2 Policy question workflow

We designed a question workflow in our Alexa skill to help users have a clear and comprehensive understanding of the different privacy policies. The privacy policies we used in this paper come from Highmark Health, which are digital privacy policy [10] and HIPAA Authorization policy [11]. The digital privacy policy is designed for any digital services provided by Highmark Health while HIPAA Authorization policy is more focused on users’ personal protected health information.

Figure 1 shows a basic structure of our policy question workflow. We extracted certain questions from the privacy policy. For each question, users can answer “yes” to agree and bring them to the next question, and users can also say “no” to disagree to the question and end the consent session. What’s more, users can also say “more details” to obtain more information about the current question, to figure out what exactly the question is asking for. Considering the time and unusability, we could not offer too many details for all of the questions or statements. To solve it, we provided detailed contact information of Highmark Health for users to let them ask for help if they want a more detailed explanation. This step is at the end of the question workflow for each question.



Flowchart - Highmark consent interface sample questions
Freya MI | November 11, 2020
Start
User could ask Alexa to review/modify privacy settings
Alexa ask the user following privacy option questions
Process other questions in the similar logic
Go through all of the questions and finish privacy settings session
Q1: Can Highmark Health disclose your protected health information, aka PHI?
NO
YES
More Details
Explain what is PHI (protected health information)
Explain how Highmark may use or disclose PHI
If you have any more questions, please call our customer service at 1-800-241-5704 with your member ID handy.
Q2: Can Highmark Health disclose your PHI to its business partners, including but not limited to Amazon?
Explain how Highmark Health is collaborating with third companies
Q3: Can Highmark Health share your information with third parties when they may not subject to certain regulations isame as Highmark Health?
Q4... Can we ......
Explain ......
Customer Service
End/Agree
End/Disagree

Fig.1 Highmark Consent Interface Sample Questions Flowchart

3.1.3 Alexa Skill Commands

We designed certain commands to meet the needs of the user to interact with the skill. These commands include letting the user complete various requests, such as turning on Highmark assistant, agreeing and authorizing privacy rules, requesting, or setting personal permissions. Table 1 shows the full commands library of our skill.

Commands	Descriptions
Open Highmark assistant	This command is used to turn on the Highmark assistant so that the user can make a request to Alexa.
Listen / Written	In order to give users a better experience, Highmark Assistant provides users with different forms of consent and authorization. Users can say "Listen" to choose the corresponding privacy policy in the form of voice question and answer review and agree/disagree. In addition, users can say "Written" to choose the way that Alexa pushes cards to the client (Alexa App) for written text reading to review and agree/disagree with the corresponding privacy policy.
I agree / I disagree	When the user chooses the text-reading format review and agree/disagree corresponding privacy policy, if the user answers "I agree", it means agreeing to the corresponding privacy terms, on the contrary, the user answers "I disagree", it means disagreeing with the corresponding privacy Terms. Once the user disagrees, the related service cannot be used, that is, Highmark Assistant cannot efficiently respond to the user's request.
Yes / No / More details	When the user chooses the form of voice question and answer review and the corresponding privacy policy of agree/disagree, for each sub-term, if the user answers "Yes", it means that they agree to the terms; if the user answers "No", it means that they do not agree to the

	terms. Once the user disagrees, the related service cannot be used, that is, Highmark Assistant cannot efficiently respond to the user's request; if the user answers "More details", Highmark Assistant will provide a more detailed explanation of the terms.
Digital privacy policy	The function of this command is to trigger Alexa to submit a review and configuration of a privacy policy request to the user.
HIPAA authorization	The function of this command is to trigger Alexa to submit a review and configure a post-password privacy policy request to the user. The main content is how Highmark collects, uses and discloses users' protected health information (PHI) while complying with HIPAA privacy rules.
Stop	This command is used to terminate or close the Highmark assistant skill
Revoke personal permissions	Users can command Highmark assistant to clear or cancel their original personal permissions by saying "revoke".

Table.1 Commands library for our Alexa skill

3.1.4 Two-Scenario Services

Our Amazon Alexa skill is able to offer different services for users with or without linking their Highmark Health account. After users enable our skill in their Alexa app, they are able to use the general services of the skill. These services are included but not limited to answering certain difinational questions, for example, users may ask the skill “What is a copay?”. This kind of service does not request any Highmark related information from users so that users can access this functionality without linking their Highmark Health account. The only thing users need to do is to agree to the digital privacy policy we mentioned in section 3.1.2.

On the other hand, the personalized services offered by our skill will require users to link their Highmark Health accounts. This feature allows users to access their personal health insurance information with Highmark Health via our Alexa skill. For example, when a user asks the skill about “what is my deductible?”, the skill is able to provide the answer based on the user’s health insurance details. Due to the HIPAA, this kind of information belongs to protected health information so Highmark Health built a corresponding policy which is HIPAA Authorization policy (3.1.1). A User needs to first agree to this policy to use the personalized feature after linking the account.

3.1.5 Personal Permission Settings

We also consider a situation that different users may have different privacy expectations for different information in health insurance. For example, one user may feel comfortable letting our skill know his or her deductible number but feel bad if our skill accesses his or her primary doctor’s information.

Thus, besides the consent and authorization interface and the two-scenario services, our skill also allows users to configure their own permission settings via voice and they can revoke all their settings at any time.

After a user links the account and agrees to the HIPAA Authorization policy, he or she may be asked to give our skill the permission for each personalized question. For example, if the user asks “what is my deductible?”, our skill will speak out a permission question which is “Can this skill access your deductible data to offer the service?” to the user. Based on the user’s answer, our skill will choose to access this kind of information or not. We promise that we will not access the data if the user answers “no” to the permission questions. For usable purposes, our skill will remember the permission and will not ask it again next time.

We also allow users to change their minds at any time. Users can revoke their permission settings at any time by simply saying “revoke privacy settings”. After that, all the privacy settings will be erased and our skill will not access the data until users give permission again next time.

3.2 User Study

We adopted a semi-structured interview method to allow participants to truly use our skills to discover innovations and problems.

3.2.1 Recruitment

We recruited 12 participants to take part in our interview research. The product we have developed is a Consent and Authorization Interface based on voice assistants, which is related to medical insurance and is targeted at a very wide range of groups. Therefore, it is necessary to recruit participants from different ages, different genders, different educational backgrounds, different occupations, etc., so that we can collect feedback from diverse groups of people.

Since it is not possible to do one-to-one in person interviews during the Covid-19 period, we adjusted it to a 20-minute online virtual interview, using the popular conference software Zoom as the interview medium. The interview will give each participant $10 as compensation.

We posted the recruitment advertisement on the Craigslist platform, and required participants to fill in a screening survey to facilitate screening of qualified and diverse participants. Participants must be over 18 years old, be in the United States, be able to speak English fluently, meet equipment and network conditions, and have experience in using voice assistants, such as Google Home, Amazon Alexa, Apple Siri, etc. In addition, with the consent of the participants, we collected some basic demographic data such as name, email address, age, education, occupation, etc. for data analysis.

3.2.2 Sample Request Questions

We have designed four sample questions, and participants can ask Alexa to get the corresponding answers. These questions are divided into two categories. One is suitable for users without linking their accounts. The Highmark assistant can make general responses to such questions and does not involve personal data. The other category applies to users with accounts linked. Highmark assistant provides a more comprehensive and customized service based on the user's personal information and health data. Regardless of whether it is before or after login, as long as the user asks Highmark Assistant, he or she needs to agree to the relevant privacy policy. In the unlogged state, the user needs to agree to the Digital Privacy Policy. After the highmark account is successfully connected, the user needs to agree to the Digital Privacy Policy and HIPAA Authorization Policy to meet HIPAA's laws and regulations regarding PHI.

Belows are the sample request questions we designed for participants:

- Request questions before linking account

a. What is a copay?
b. What is Medicare?

- Request questions after linking account

c. What is my deductible?
d. What is my primary doctor?

3.2.3 Dummy Highmark Application

To simulate the situations more realistically, we developed a dummy Highmark Website, which only provides sign up account and sign in account functionalities. The participant could assume he/she is the Highmark insurance holder and has signed up an account for this Highmark application. In this way, the participant could try to link his/her account via login page and redirect back to the “linking account successfully” page to tell Alexa and the participant that the account has been connected. Then the participant would simulate the requests and tasks of “after logged in” mode.

3.2.4 Interview Process

Every qualified participant needs to fill out a screening survey before the interview. Before the formal situational test, the interviewer will ask the participants their knowledge of medical insurance and their proficiency with the voice assistant. If necessary, they need to explain or simulate how to interact with the voice assistant. At the same time, participants were asked whether they have privacy concerns about the voice assistant, and the participants’ privacy awareness was evaluated.

Due to the inconvenience of the virtual interview, we need to explain to the participants that we completed the task by sharing the screen of the Alexa Developer Console, combining typing requests and voice. At the same time, provide and explain all command words and simulated sample questions to participants.

Participants need to experience two scenarios in order. The first scenario is to ask Alexa some general questions and review the digital privacy policy via voice format or written format. After the participant has used the skill for a while, he/she would be more familiar with the commands and might need to get more answers from customized questions. Then the second scenario will require the participant to link his/her highmark account to the Highmark assistant skill to complete these more complex questions like “what is my deductible?”. Before answering these questions, the participant needs to review and agree to the HIPAA Authorization Privacy Policy and also give the permission of getting specific personal information to the Highmark assistant skill. The participants could revoke or reset the personal permission settings to the default (the default is not allowing HIghmark to get any personal information).

4. Interview Result

We interviewed 12 participants in total and gathered valuable feedback from the participants. 9 out of 12 participants agreed that the voice assistant is meeting their expectations and will use them if the software is on the market. According to the feedback, we categorized them into three major sections: privacy-related feedback, usability-related feedback and other feedbacks.

4.1 Privacy aspects

Half of the interviewees expressed that they feel their privacy is respected and protected by the skill, and one user described his experience as: “I never pay attention to the privacy options before when using a voice assistant. The functions in this software help me to customize and evaluate my privacy and are really useful”. Since we are using a concentrated version of privacy policies, users have a better chance to be informed about the content: 3 participants expressed that they never read a privacy policy before but since this concentrated version can save their time when going through it, they are informed about the content of it. Compared to common privacy policies, fine-grained questions are more concise and easier to understand. Two interviewees said they have more knowledge about privacy after using our prototype Alexa skill. Since our Alexa skill supports data access revoking at any time, the majority of interviewees think that this function provides them more control over their own data. Overall, participants are satisfied with the privacy aspects of our prototype software and feel they are more respected and protected compared to other voice assistant applications.

However, the participants do mention certain limitations on our skill. Many of them are confused about why the skill has two policies: one HIPAA policy and one digital policy and why this is necessary. Two users said they do not really care about privacy and find the option setting sections annoying: they want to start using the skill as soon as possible. Since the users have the rights to revoke any consent at any time, they expect to be notified about this rule before everything instead of after choosing the options

4.2 Usability aspects

Account-linked customized functions provided a customized user service user experience and all participants agreed that a customized service indeed made the skill more usable.

Participants pointed out several usability problems. Since the prototype we used during the user study is developed in a short period of time and works as an Alpha version, these problems are expected. In future work, the usability of the software is expected to be enhanced. Especially, for the “more detail” option, many aspects can be improved: Users are expecting to hear the title of the “more details” option (e.g. more details about ad personalization options using location data) and in some cases, the details take up to 1 minute to read, which is considered too long for some users. During the voice delivering progress, some users wish to switch between text notification and voice instead of sticking to the same one for the whole progress. Some users expected to hear different interactions from the voice assistants instead of asking the same question of “what’s your next request” after each statement. When making choices, some users wish to have an additional confirmation step before the option is recorded. A repeat option shall be added to the interaction process in case the user misses some words. Some users disagreed with one or more consent requirements and found themselves needing to restart the whole process again once they changed their minds. Users are expected to be acknowledged that those are necessary for running the software and they have to agree in order to use it before the consent processes start. Due to the limitation of OAuth account linking function provided by AWS, the skill is required to restart after an external account has been linked. Some users are not satisfied with that.

4.3 Other aspects

A third of the participants think that setting privacy options over voice is an innovative idea and they are keen to try it out once it is on the market. One user pointed out that the user study can be more engaging with more realistic scenarios instead of using pre-set tasks and questions. One user thinks that using a mobile application is enough thus a voice assistant is not necessary. Some users have limited experience on voice assistants before and they are not sure about the process of voice consent. They may think reading a text version of the policy is faster than delivering it via voice. Some users are worried about the legalization aspect of the software: since the voice assistant will not verify the identity of the speaker, anyone who has the access to the device will be able to manipulate the settings.

5. Discussion

5.1 Prototype evaluation

According to our user study, The majority of the users agree that the product protects and respects their privacy more than average application and are willing to use the product if it is on market. The application helps the users to be informed about the HIPAA and digital policy even for some those who hardly read any privacy policies before. The software gives users full control over their data. Interactions are delivered via the voice interface successfully.

Thus, it's safe to say our Alexa skill prototype proves that using healthcare applications over voice assistants and maintaining user privacy is feasible and practicable.

5.2 Limitations

During the entire development and user study process, there are indeed certain limitations. On the one hand, due to the limitation of time, the skill we developed is a proof of concept and cannot fully represent a commercial level product. We put more concentration on the consent and authorization process through voice. Although the skill can offer certain different services for users' requests, the purpose of the services we implemented is to distinguish whether users are linked accounts. The skill itself does not provide the whole functionality as a health insurance voice assistant app. On the other hand, the user study sample is rather small and might be potentially biased since it may not fully represent the user group, and also, we interviewed the participants via Zoom call and screen sharing. The user experience under this situation might be different from actual user scenarios when users talk with the voice assistants directly.

5.3 Future Works

One of the potential future works would be to continue the development of the Alexa skill. Our skill is open-sourced on Github for potential researchers in the future to continue our work. As we have discussed some of the limitations and feedback from our interviewees, some of the takeaways can be easily integrated into the current version and improve the usability of the skill greatly.

Besides, one can easily extend the study beyond the scope of just developing a skill for our sponsor Highmark Health. In fact, we conducted the study with extensibility in mind, and most of our works are not limited to applying for Highmark Health solely, but for healthcare privacy in general. We have presented a general voice interface for consent and authorization, and other healthcare app developers can adopt the same paradigm and integrate it into their products as well.

6. Conclusion

In this paper, we introduced an Amazon Alexa skill with a consent and authorization interface. This innovative consent and authorization interface offers a two-way privacy policy delivery method - that is, it can not only let users read a written version of the policy but also can speak out the summary questions of the policy to users. For this listening delivery way, we designed a multi-level summary question workflow in order to give users a comprehensive understanding of the policy through voice. Our sponsor, Highmark Health, has two types of privacy policy for users with or without linking their Highmark accounts to the third party digital service so that our skill also offers general service for users who don't link their accounts and personalized service for users with accounts linked. Our skill also allows users to configure their own personal permissions for different types of their PHI to enhance the controllability over their personal data. We believe this novel method of voice consent and authorization will give users a new interactive experience with privacy policy, and may lead to more focus on the research in the field of voice consent. Finally, we also conducted 12 semi-structured interviews and collected feedback on our prototype skill. These feedbacks can help guide our future improvement of the skill and other research in this field.

Reference

[1]Littenberg, B., &amp; Maclean, C. D. (2006). Passive consent for clinical research in the age of HIPAA. Journal of General Internal Medicine, 21(3), 207-211. doi:10.1111/j.1525-1497.2006.00339.x

[2]Cunche, M., Métayer, D., &amp; Morel, V. (2018, December 17). A Generic Information and Consent Framework for the IoT. Retrieved September 24, 2020, from https://arxiv.org/abs/1812.06773

[3]Requirements for Skills that are HIPAA-Eligible. Retrieved September 24, 2020, from https://developer.amazon.com/en-US/docs/alexa/custom-skills/requirements-for-hipaa-eligible-skills.html

[4] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers. Proc. ACM Hum.-Comput. Interact. 2, CSCW, Article 102 (November 2018), 31 pages. DOI:https://doi.org/10.1145/3274371

[5] Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, David Wagner, and Serge Egelman. Privacy Attitudes of Smart Speaker Users.Proceedings on Privacy Enhancing Technologies (PoPETS), 2019(4).

[6]Hu, Hongxin, and Christin Wilson. Dangerous Skills Got Certified: Measuring the Trustworthiness of Amazon Alexa Platform. Sept. 2020.

[7] Rawes, Erika and Wetzel Kim. “What is Alexa? Where does she come from? How does she work?”, Retrieved November 10, 2020, from https://www.digitaltrends.com/home/what-is-amazons-alexa-and-what-can-it-do/.

[8] Ovenden, James. “How Amazon Alexa Works. The technology behind the machine learning device.”, Retrieved November 10, 2020, from https://channels.theinnovationenterprise.com/articles/how-amazon-alexa-works.

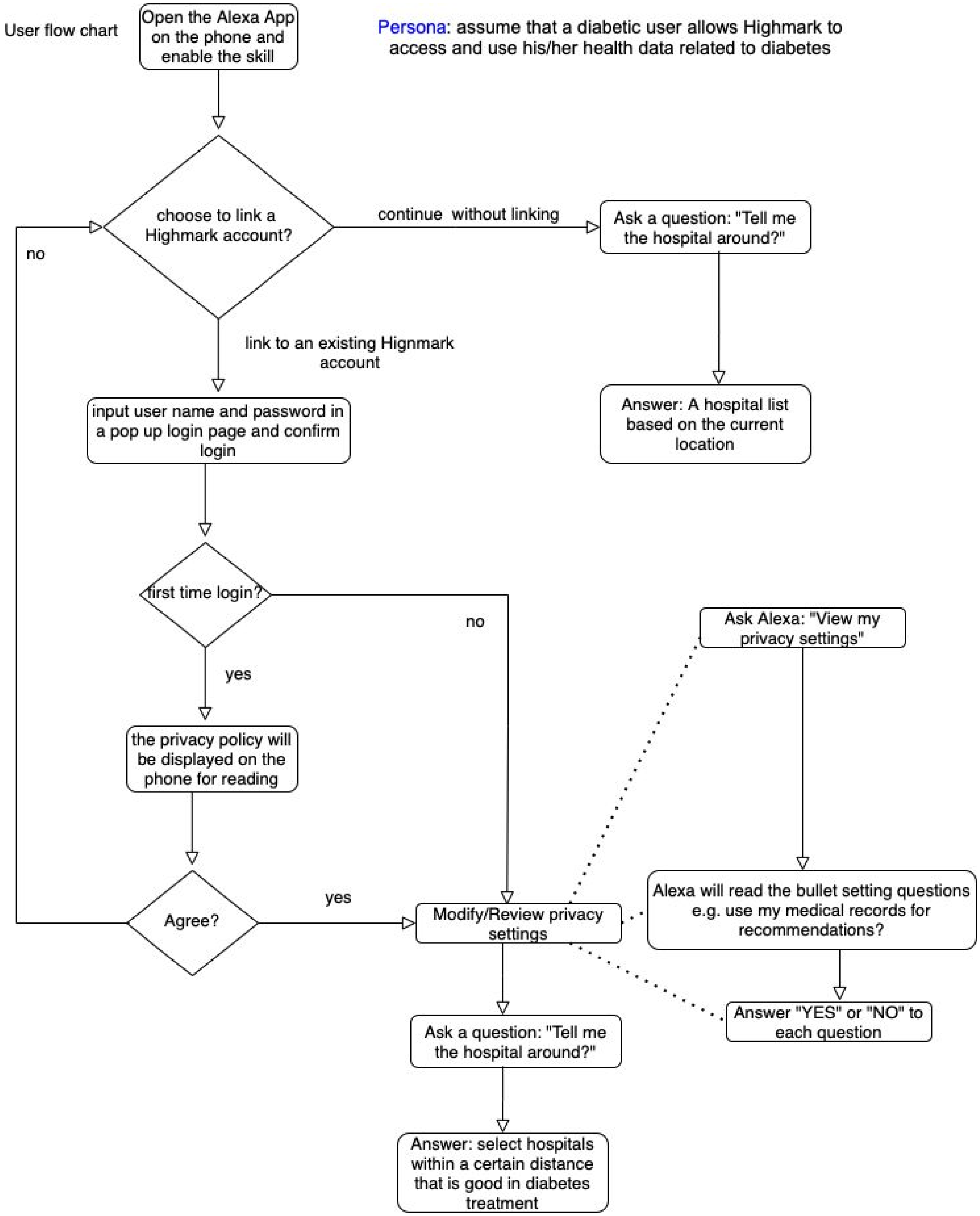
[9] “Resources to Build with AVS.”, *Amazon Alexa*, Retrieved November 10, 2020, from https://developer.amazon.com/en-US/alexa/devices/alexa-built-in/development-resources.

[10] “Highmark's Privacy Policy.”, *Highmark Health*, Retrieved November 10, 2020, from https://www.highmark.com/privacy.html.

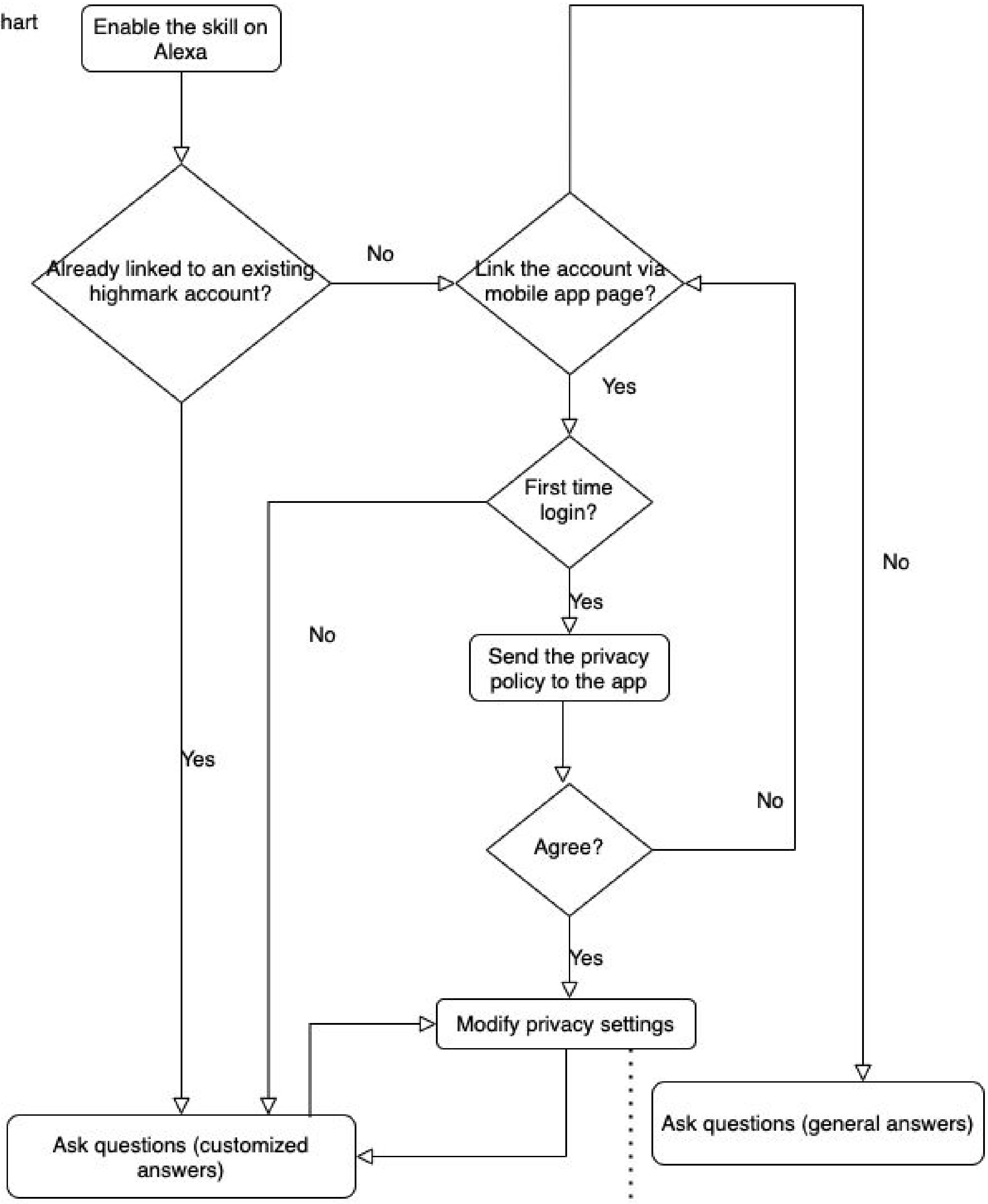
[11] “Digital HIPAA Authorization – Retail Health/Customer Journey.”, *Highmark Health*, Retrieved November 10, 2020, from https://cdn.highmark.com/content/global/policies/Digital_Channel_Consent_05.04.2020.pdf.

Appendix

User / Technical flow charts


User flow chart
Open the Alexa App on the phone and enable the skill
Persona: assume that a diabetic user allows Highmark to access and use his/her health data related to diabetes
choose to link a Highmark account?
continue without linking
Ask a question: "Tell me the hospital around?"
no
link to an existing Hignmark account
Answer: A hospital list based on the current location
input user name and password in a pop up login page and confirm login
first time login?
no
Ask Alexa: "View my privacy settings"
yes
the privacy policy will be displayed on the phone for reading
Alexa will read the bullet setting questions e.g. use my medical records for recommendations?
yes
Agree?
Modify/Review privacy settings
Answer "YES" or "NO" to each question
Ask a question: "Tell me the hospital around?"
Answer: select hospitals within a certain distance that is good in diabetes treatment

Tech flow chart


Enable the skill on Alexa
Already linked to an existing highmark account?
No
Link the account via mobile app page?
Yes
First time login?
Yes
No
Send the privacy policy to the app
No
Yes
Agree?
No
Yes
Modify privacy settings
Ask questions (customized answers)
Ask questions (general answers)

In the process of modifying the privacy settings:

1. Abstract the corresponding questions from the privacy policy and service terms of Highmark Health.
2. Hand questions to Alexa to read them.
3. After hearing each corresponding question, the user can choose to answer "yes" and "no".
4. Alexa sends the results(answers) back to the back-end, and the back-end saves the user's customized privacy settings.

Digital Privacy Policy Extracted Questions

○ **Can Highmark Health collect your basic information via online forms?**

- Yes: Go to the next question
- No: End the consent session
- More details:

    Highmark Health invites users to contact us using inquiry forms available on our corporate-owned platforms for account questions or to learn more about our products and services. The personal information we request on inquiry forms generally includes your name, address, phone number, email address, and the details of your inquiry. We may use such information to review and respond to your request or communication, or use contracted service providers to do that for us.

    - Yes: Go to the next question
    - No: End the consent session
    - More details:

        If you have more questions about this Online Privacy Policy, or concerns regarding your personal information, please contact us by emailing "privacy@highmarkhealth.org" or calling 1-866-228-9424.

○ **Can Highmark Health collect your secure portals?**

- Yes: Go to the next question
- No: End the consent session
- More details:

    Highmark Health has established secure portals for use by members and patients. When you access them to review your health and benefit-related information or to contact your health plan or physician's office regarding certain inquiries, such as reviewing claims or requesting prescription refills, we collect certain personal information, such as your user ID and password, IP address, click streams, and cookie ID.

    - Yes: Go to the next question
    - No: End the consent session
    - More details:

        Communications sent by or to members or patients who choose to use these secure portals may also be recorded in transaction logs to monitor content, compliance with applicable law and regulations, or functionality of the services. If the information collected is deemed to be PHI as noted above, its use and disclosure will be subject to HIPAA and an applicable NPP.

        - Yes: Go to the next question
        - No: End the consent session
        - More details:

If you have more questions about this Online Privacy Policy, or concerns regarding your personal information, please contact us by emailing "privacy@highmarkhealth.org" or calling 1-866-228-9424.

○ **Can Highmark Health collect your information via interactive chat?**

- Yes: Go to the next question
- No: End the consent session
- More details:

  Our consumer platforms may offer interactive chat technology to assist users. That interactive technology may collect personal information such as name, date of birth, address, and account number for authentication purposes or to provide specific plan benefit details in a personalized response. It may also capture session-related information such as web logs to document the interaction. If the information collected is deemed to be PHI as noted above, its use and disclosure will be subject to HIPAA and an applicable NPP.

  - Yes: Go to the next question
  - No: End the consent session
  - More details:

    If you have more questions about this Online Privacy Policy, or concerns regarding your personal information, please contact us by emailing "privacy@highmarkhealth.org" or calling 1-866-228-9424.

HIPAA Authorization Extracted Questions

○ **Can Highmark Health disclose your protected health information, aka PHI?**

- Yes: Go to the next question
- No: End the consent session
- More details:

  Your PHI is including but not limited to information maintained in my health plan's member portal such as policy number, co-pay, co-insurance, and deductible information, dates of service, and claims information, and any information you freely share through the two-way chatbot interface.

  - Yes: Go to the next question
  - No: End the consent session
  - More details:

    To offer this personalized experience, Highmark Health must collect, use, and disclose personal information across our digital tools and channels. This information can include, among other things, demographics such as your name and date of birth, contact information such as phone number, address, and email address, details about receipt of healthcare services such as dates of service and medical conditions and procedures, details about your insurance benefits such as policy number and claims, and information about your activities on our digital tools and channels such as internet protocol address, device identifier, and cookie ID.

- Yes: Go to the next question
- No: End the consent session
- More details:

  If you have any more questions, please call our customer service at 1-800-241-5704 with your member ID handy.

○ **Can Highmark Health disclose your PHI to its business partners, including but not limited to Amazon or Google, for purposes of supporting the Program. This Authorization will remain in effect until you revoke it by notifying Highmark Health in writing as specified herein?**

- Yes: Go to the next question
- No: End the consent session
- More details:

  Highmark Health is collaborating with companies including Amazon on digital improvement projects supporting the Program. Our collaborations allow us to offer capabilities such as real-time chat sessions where users can ask questions on our member portal like “have I met my deductible this year” and similar inquiries. These projects require that Highmark Health share your Personal Information with its business partners (like Amazon) for product and solution development, testing, and refinement purposes.

  - Yes: Go to the next question
  - No: End the consent session
  - More details:

    If you have any more questions, please call our customer service at 1-800-241-5704 with your member ID handy.

○ **Can Highmark Health share your information with these third parties when they may not subject to certain federal and/or state privacy and security laws and regulations in the same manner, or to the same degree, as Highmark Health?**

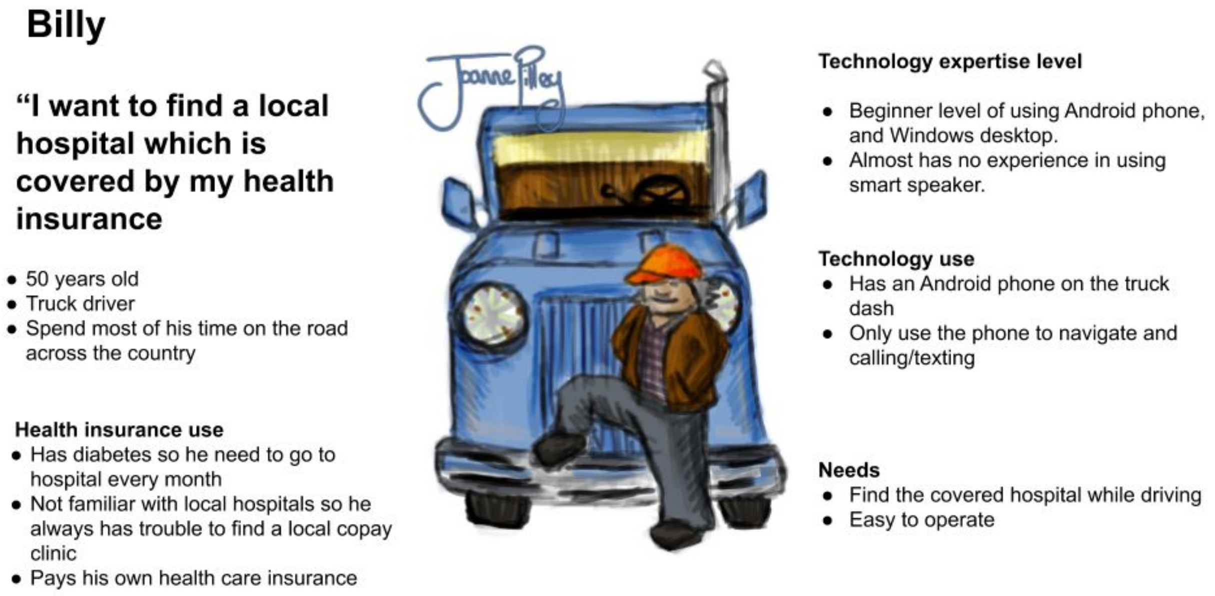
- Yes: Go to the next question
- No: End the consent session
- More details:

  Highmark Health recognizes that its business partners may not be subject to the same range of federal and/or state laws governing the collection, use, and disclosure of Personal Information. Nevertheless, we have taken a number of steps to ensure that your information is handled responsibly, such as by maintaining a rigorous internal privacy and data ethics program, negotiating restrictive contract terms with third party service providers, and seeking to obtain your affirmative authorization, as applicable.

- Yes: Go to the next question
- No: End the consent session
- More details:

  If you have any more questions, please call our customer service at 1-800-241-5704 with your member ID handy.

Personas



Billy

"I want to find a local hospital which is covered by my health insurance

- 50 years old
- Truck driver
- Spend most of his time on the road across the country

Health insurance use

- Has diabetes so he need to go to hospital every month
- Not familiar with local hospitals so he always has trouble to find a local copay clinic
- Pays his own health care insurance

Technology expertise level

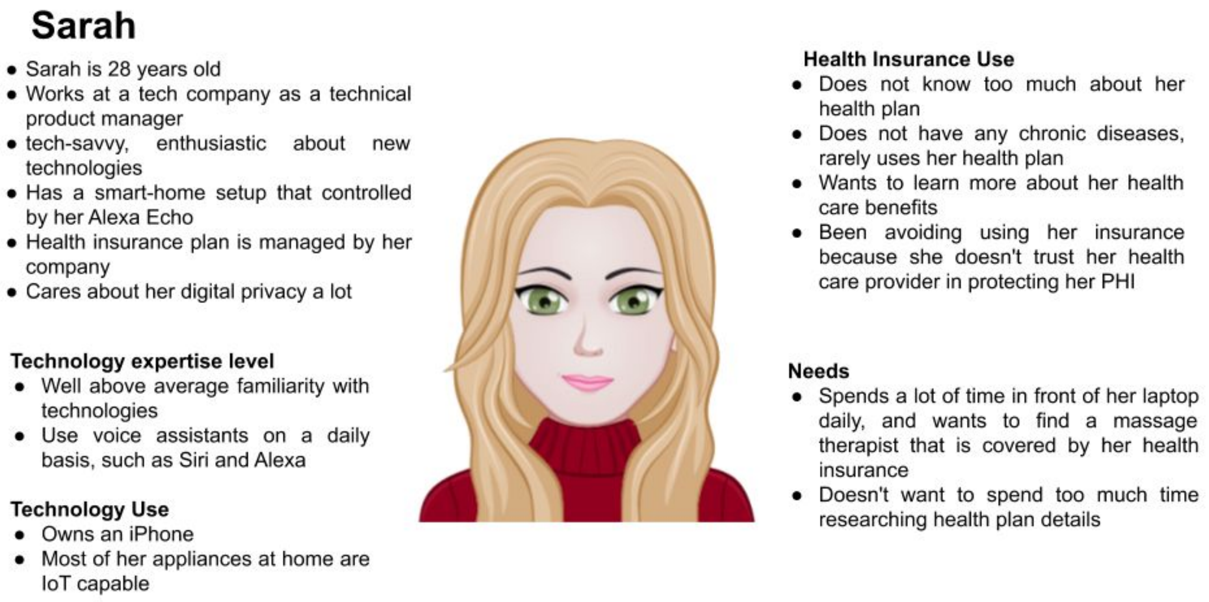
- Beginner level of using Android phone, and Windows desktop.
- Almost has no experience in using smart speaker.

Technology use

- Has an Android phone on the truck dash
- Only use the phone to navigate and calling/texting

Needs

- Find the covered hospital while driving
- Easy to operate



Sarah

- Sarah is 28 years old
- Works at a tech company as a technical product manager
- tech-savvy, enthusiastic about new technologies
- Has a smart-home setup that controlled by her Alexa Echo
- Health insurance plan is managed by her company
- Cares about her digital privacy a lot

Technology expertise level

- Well above average familiarity with technologies
- Use voice assistants on a daily basis, such as Siri and Alexa

Technology Use

- Owns an iPhone
- Most of her appliances at home are IoT capable

Health Insurance Use

- Does not know too much about her health plan
- Does not have any chronic diseases, rarely uses her health plan
- Wants to learn more about her health care benefits
- Been avoiding using her insurance because she doesn't trust her health care provider in protecting her PHI

Needs

- Spends a lot of time in front of her laptop daily, and wants to find a massage therapist that is covered by her health insurance
- Doesn't want to spend too much time researching health plan details

Recruiting Post

CMU Healthcare Consent Interface study is searching participants - Zoom interview, $10, 15-20 minutes

We are a research team from Carnegie Mellon University and plan to find people to participate in the virtual interview study via Zoom who are as representative as possible of the US population. In the interview, we will simulate the healthcare consent interface to the participant and ask about their experience and feedback. We will not acquire healthcare-related information or any other personal sensitive information from participants.

To be eligible for this study, you must:

* Be 18 years of age or older

* Be located in the U.S. at the time of the interview

* Be fluent in English

* Have a desktop or laptop computer and a high-speed and stable internet connection to use for the interview, and be able to install and run Zoom on that computer (we can assist you to do this)

* Have experience in using a voice assistant like Siri, Alexa, Google Home, etc.

Participants will receive a $10 Amazon gift code for participating.

If you wish to participate, please fill out the quick screening survey at the link below, and if you are eligible, we will contact you with more information:
http://cmu.ca1.qualtrics.com/jfe/form/SV_7UMpIYv27fp6lut
You can also contact us by email (fangxiam@andrew.cmu.edu) to express interest or ask questions about the study.

Screening survey

Start of Block: Introduction

We are a research team from Carnegie Mellon University, and plan to find people to participate in the virtual interview study via Zoom who are as representative as possible of the US population. We will use the following questions to select a diverse group of participants in terms of age, gender, location, education and subject-matter expertise. In the interview, we will simulate the healthcare consent interface to the participant and ask their experience and feedback. We will not acquire healthcare related information or any other personal sensitive information from participants.

If you are interested in participating in our interview study, please complete this screening & demographic survey, it should just take a few minutes.

If you are selected for the interview study, a member of the research team will reach out to you via email to schedule an interview on Zoom in October to November 2020. The virtual interview will take about 15-20 minutes. Each participant who completes the interview will receive a $10 Amazon gift code via email.

If you do not go on to participate in the interview study, this data will be deleted when the recruitment process has ended. If you consent to participate in the interview portion of the study, we may store this data (anonymized, not with identifying information such as your name or email address) and use it when analyzing and reporting the results from our interview data.

End of Block: Introduction

Start of Block: Remote Study Eligibility

1. Are you 18 years older?

○ Yes

○ No

2. Are you located in the United States?

○ Yes

○ No

3. Do you have access to a computer with a fast and stable network for the virtual interview?

○ Yes

○ No

4. Are you able and willing to install Zoom on that computer and use it for the virtual interview?
   If you need any help, please let us know and we'll be happy to help.

○ Yes

○ No

5. Can you speak English fluently?

○ Yes

○ No

6. Have you used voice assistants like Alexa, Siri, Google Home etc. before?

○ Yes

○ No

7. If you have any questions or comments about the study, please leave them here.

____

____

End of Block: Remote Study Eligibility

Start of Block: Highmark Demographics

1. What is your age range?

○ 18-30 years old

○ 31-45 years old

○ 46-60 years old

○ 61+

2. How do you describe your gender identity?

□ Male

□ Female

□ Agender

□ Non-binary

□ Genderqueer

□ Not sure

□ Not listed above (you may describe if you wish) ____

□ Prefer not to respond

3. What is the highest level of school you have completed or the highest degree you have received?

○ Less than high school degree

○ High school graduate (high school diploma or equivalent including GED)

○ Some college but no degree

○ Associate degree in college (2-year)

○ Bachelor's degree in college (4-year)

○ Master's degree

○ Doctoral degree

○ Professional degree (JD, MD)

○ Prefer not to respond

4. Do you have a formal education in any of the following fields?

   ("Formal education" could mean a completed degree or certificate, or classes or training you took towards a degree or certificate.)

□ Computer-related fields (e.g., computer science, computer engineering, programming, development, IT)

□ Law or legal services

□ Healthcare practice (e.g., medical assistant training, nursing school, medical school)

□ Healthcare administration

□ None of the above

End of Block: Highmark Demographics

Start of Block: Contact information

5. What is your preferred name ?

   This is required if you wish to participate, since this is how we will contact you to provide more information and schedule an interview.

   Your name will be stored securely and will not be used for any purposes other than recruitment, scheduling, and payment for this study.

____

6. What is your primary email address?

   This is required if you wish to participate, since this is how we will contact you to provide more information and schedule an interview.

   Your email will be stored securely and will not be used for any purposes other than recruitment, scheduling, and payment for this study.

____

End of Block: Contact Information

Interview scripts

1. Do you use voice assistants frequently?
2. If you use voice assistants, any concerns you may have while you are using them?
3. Do you have health insurance? Do you use mobile applications developed by your healthcare provider to manage your health plan?

=> Yes: Do you have any privacy concerns over managing your health related information on your mobile phone? Do you trust your health care provider in managing your personal health information?

=> No: Why not?

4. Have you ever asked your voice assistants about any personal health related questions?
5. Have you used voice assistants for healthcare related questions, such as asking questions about your health insurance plan or reminder of taking medicine?
6. User testing: go through all of the questions and consent process with participants, simulating the scenario of patients using our health care consent interface.
   Questions:
   - How is your general experience of using the interface?
   - Are you satisfied with the approach we are sending the privacy policy?
     => No: what other approaches do you prefer, for example, via mobile phone, email, or voice?

Before Scenario 1:

Imagine you are ..., and you are a Highmark Health insurance
holder. However, you don't know too much about healthcare in general, and you would like to learn more about it. Recently, you just discovered that Highmark Health has an Amazon Alexa Skill, where you can install it onto your Alexa devices and ask it questions regarding healthcare. You are excited to try it out. Right now, you have two general questions that you would like to know the answers of:

1. What is a copay?

2. What is medicare?

You can request Alexa for these answers via asking these two questions.

After Scenario 1, before scenario 2:

You've been using the skill for a while now. Today, you just discovered that the skill has an account linking capability, where you can use your Highmark Health insurance digital account to login, letting the skill know a little bit more about your plan and information, therefore answering more complicated questions for you. You want to try it out - but first, you need to link your account. After linking your account, you would like to know: 1. What is my deductible?

2. Who is my primary doctor?

You can request Alexa for these answers via asking these two questions.