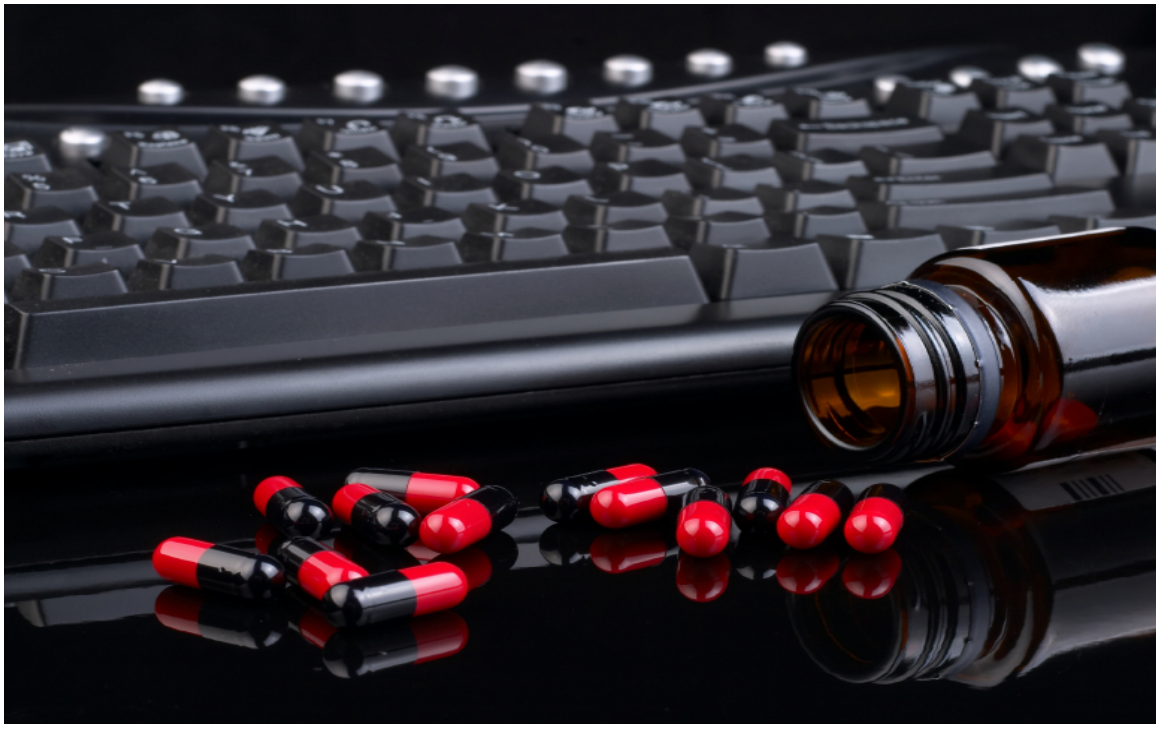
Ponemon INSTITUTE



Risks & Rewards of Online & Mobile Health Services: Consumer Attitudes Explored

Sponsored by Experian® Data Breach Resolution

Independently conducted by Ponemon Institute LLC

Publication Date: January 2014

Risks & Rewards of Online & Mobile Health Services: Consumer Attitudes Explored

Ponemon Institute, January 2014

Part 1. Introduction

The Internet and mobile apps have changed how organizations deliver services and engage with their target audiences. This is especially true for the health care industry. With access to the Internet, consumers can consult with physicians, book an appointment, check test results or learn more about a health condition.

What is eHealth?

In this study, we define online health or eHealth as health care services delivered through the Internet or mobile apps. This includes searching for health information on the Internet (i.e., WebMD) or accessing medical files from an online health care provider.

Our study, *Risks & Rewards of Online & Mobile Health Services: Consumer Attitudes Explored*, examines consumers' perceptions about sharing their personal information when using online health services and mobile apps. It also reveals the practices believed to be important to protecting personal health information from a possible data breach.

We surveyed almost 1,000 consumers who are regular Internet and mobile apps users. Their most popular online activities are emailing and texting, browsing and shopping and online searching and research. However, not all Internet savvy consumers in our study are choosing to use one of the many health and wellness services available online. In fact, 52 percent of those surveyed report they are non-users.

To better understand why certain consumers are reluctant to use eHealth services, our analysis looks at the differences in perceptions between the 48 percent of respondents who do use eHealth services and the 52 percent who do not. One key difference appears to be concerns about the privacy and security of their information.

Specifically, those choosing not to use eHealth services are more skeptical about the ability of the eHealth provider to protect personal health and wellness information entrusted to it. The 48 percent of consumers who do use one or more online health and wellness services find them to be helpful and of value. In fact, 85 percent of users predict their eHealth use will substantially increase, increase or stay at the same level over the next year.

Many users of online health services report they have been accessing these services for three or more years. Some of their most common online activities include browsing health-related Internet sites such as WebMD, accessing and reviewing their patient records, managing payments to health care insurers and monitoring fitness or weight loss programs.

Major implications of this study sponsored by Experian® Data Breach Resolution include the following:

- **Online and mobile health services are considered more risky than other online activities**. Fifty-eight percent of Internet users believe accessing their medical records online puts their personal health information at risk.
- **Data breach incidents involving mobile apps would affect use.** Sixty-one percent of Internet users would stop using their favorite mobile health app if a data breach occurred.
- **Security is more important than privacy and anonymity.** Seventy-four percent of Internet users over the age of 36 believe proper security safeguards are critical for online health services vs. 63 percent of younger users (under the age of 35). However, younger-aged respondents appear to attach more importance to anonymity rather than privacy or security (61 percent of younger users vs. 48 percent of older users).

- **Medical identity theft is a growing concern.** Fifty-six percent are either very concerned or concerned about the theft of their health-related personal information or insurance credentials.
- **Who should be responsible for protecting personal health information online?** Forty-eight percent of non-users and 39 percent of users believe government regulations are needed to protect the privacy rights of individuals. But when asked who should be responsible for the security of personal health information, 65 percent of users and 69 percent of non-users would want anyone but the government to be responsible.

Part 2. Key Findings

Following is a summary of the key findings. We have organized the report according to the following topics:

- The eHealth user experience
- The privacy and security of personal health information is held to a high standard
- The age factor in eHealth
- How to establish trust in eHealth services

The eHealth user experience

Figure 1 lists the health-related activities that eHealth users say they routinely perform online. As can be seen, browsing health websites, monitoring weight loss and reviewing medical records are the top three most frequently cited eHealth activities.

Figure 1: What eHealth users do online
More than one choice permitted

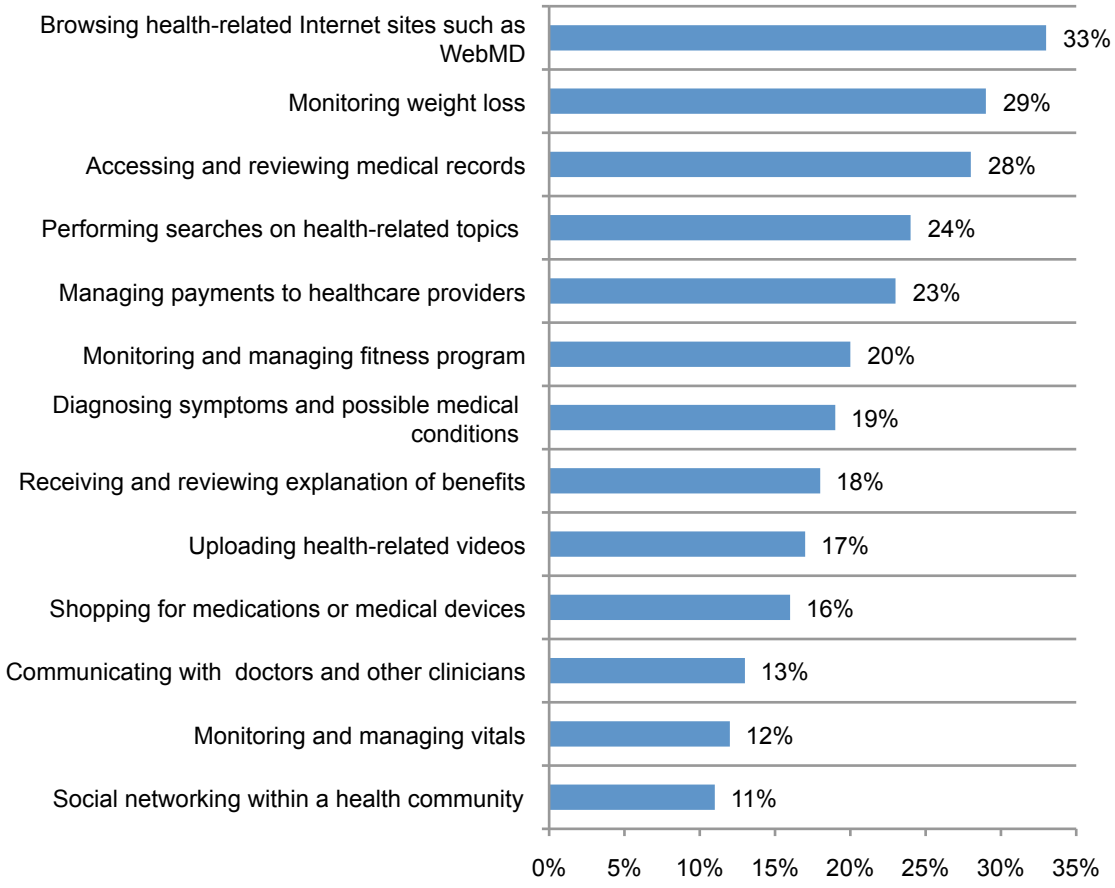
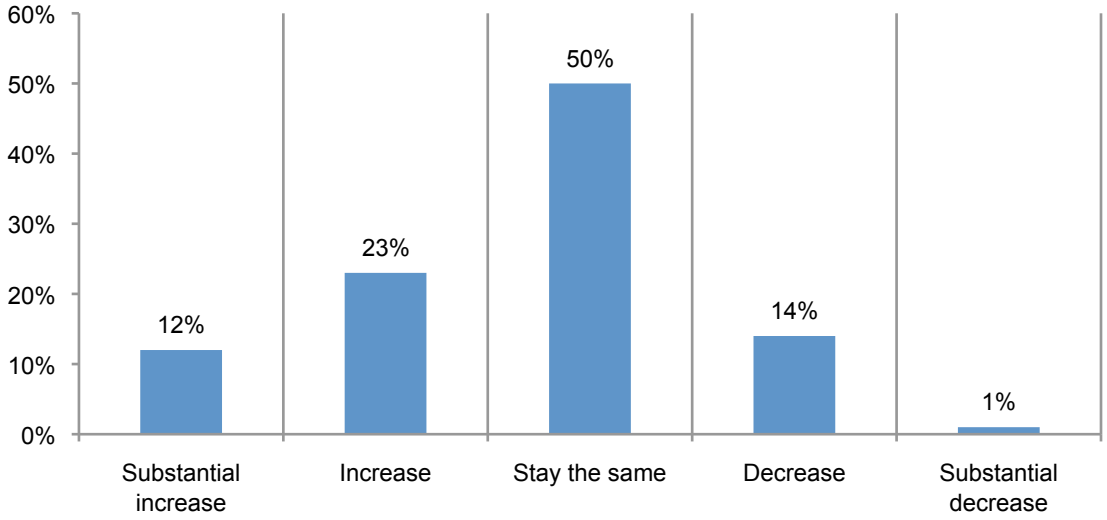


Figure 2 reports the expected use of eHealth services over the forthcoming year. These results show an expected increase of 35 (12+23) percent and only a 15 (14+1) percent decrease. About half of eHealth users say their use rates will stay the same.

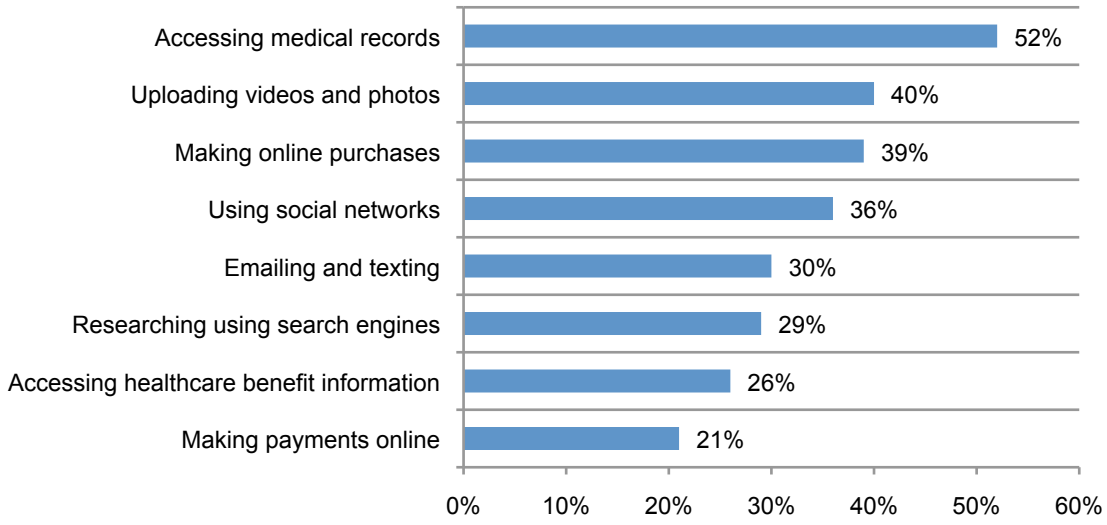
Figure 2. Will eHealth usage increase, decrease or stay the same over the next 12 months?



The privacy and security of personal health information is held to a high standard

Users of eHealth services express significant concern about privacy and security when accessing their medical records online. When asked to indicate all online activities they consider most risky, 52 percent of eHealth users say it is accessing their medical records from the Internet. Lower on the risk scale is accessing health care benefit information or making payments online.

Figure 3. Online activities that put privacy & security at greatest risk
Three choices permitted



What's more unforgivable: A data breach involving an online health service, a mobile health app or social media? Figure 4 reveals that 61 (25+36) percent of respondents say they would most likely discontinue using their favorite mobile health app if the provider had a data breach involving the loss or theft of personal information. Similarly, 58 (24+34) percent of consumers would most likely stop using their favorite online health resource such as WebMD if they reported a data breach involving personal information.

Only 36 (15+21) percent of respondents say they would most likely discontinue using Facebook, LinkedIn or other social media providers if they had a data breach involving the loss or theft of personal information.

Figure 4. Would a data breach stop the use of your favorite social media, online health services or mobile health apps?
Most likely = yes with certainty + very likely responses

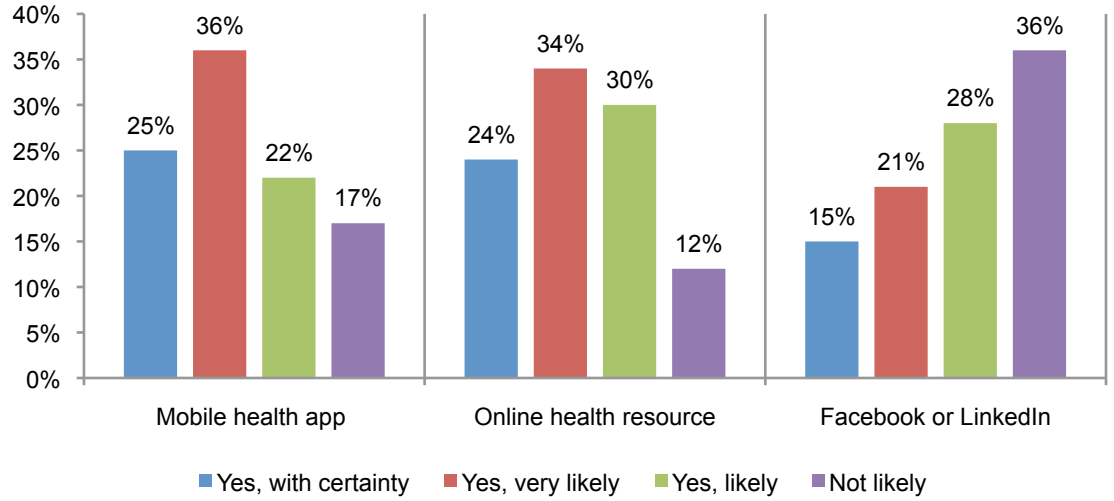
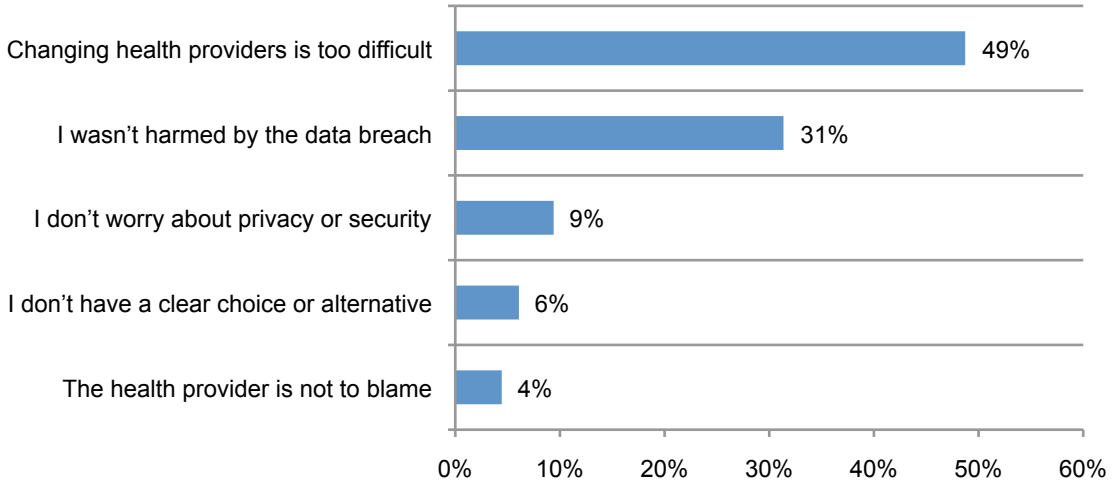


Figure 5 shows the top reasons why respondents who became victims of a data breach involving health information **did not** terminate the relationship. Forty-nine percent say it was too difficult to change health care providers. Another 31 percent believe they were not harmed. Only 9 percent say they do not worry about privacy or security.

Figure 5. Reasons for keeping a health care provider or online health service after a data breach

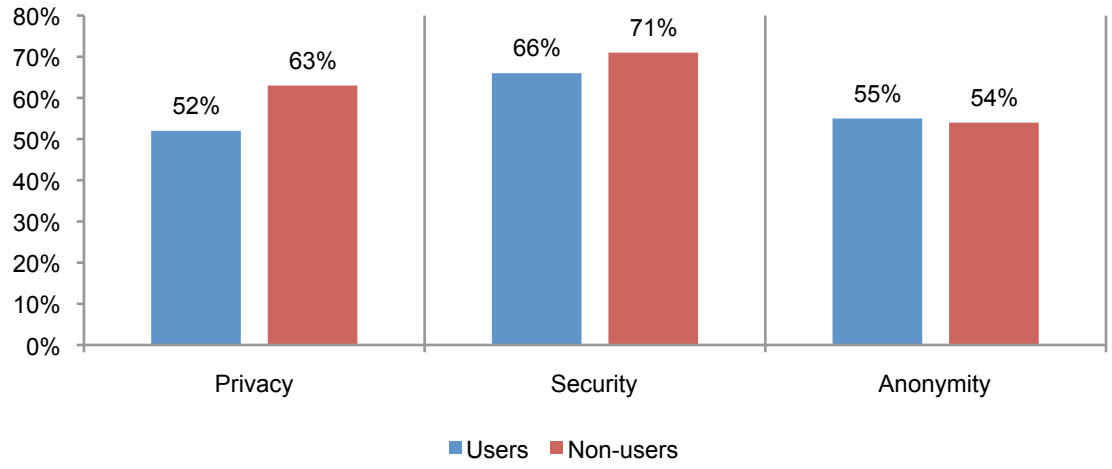


Security is more critical than privacy and anonymity in the decision to use or not use eHealth services. Sixty-nine percent of respondents say it is essential or very important that online health services have adequate security safeguards in place. This is followed by 58 percent who say privacy is essential or very important and 55 percent who say anonymity is essential or very important.

As mentioned above, the majority of respondents in this study (52 percent) do not use eHealth services or apps. To understand why they may be reluctant to use online medical services, we analyzed the differences in perceptions between users and non-users concerning the importance of privacy, security and anonymity of their personal health information.

As can be seen in Figure 6, the largest difference between users and non-users of eHealth services concerns privacy. Sixty-three percent of non-users versus 52 percent of users see privacy as essential or very important (Diff = 11 percent).

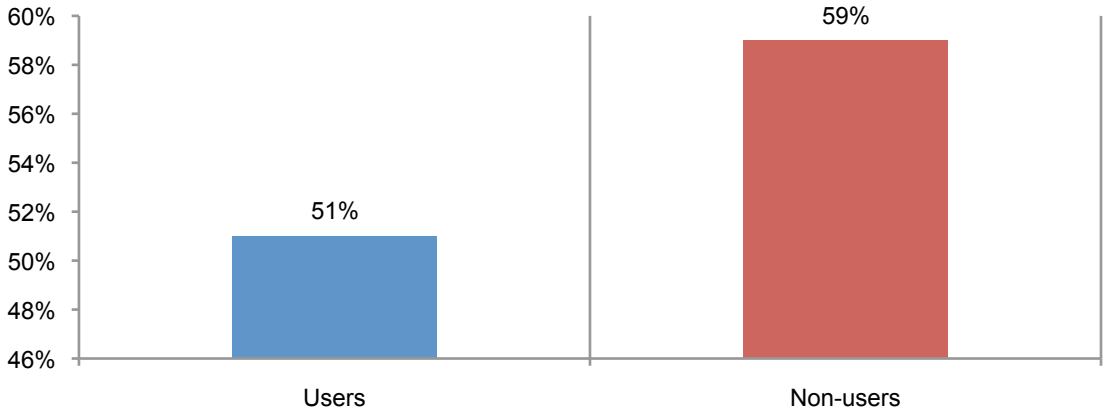
Figure 6. What factors are most important for online health services?
Essential and very important response combined



With more personal health information online, medical identity theft is a growing concern for respondents. With recent news stories about the insecurity of personal health information associated with the Patient Protection and Affordable Care Act's online registration program (a.k.a. Obamacare), worries about medical identity theft are increasing.

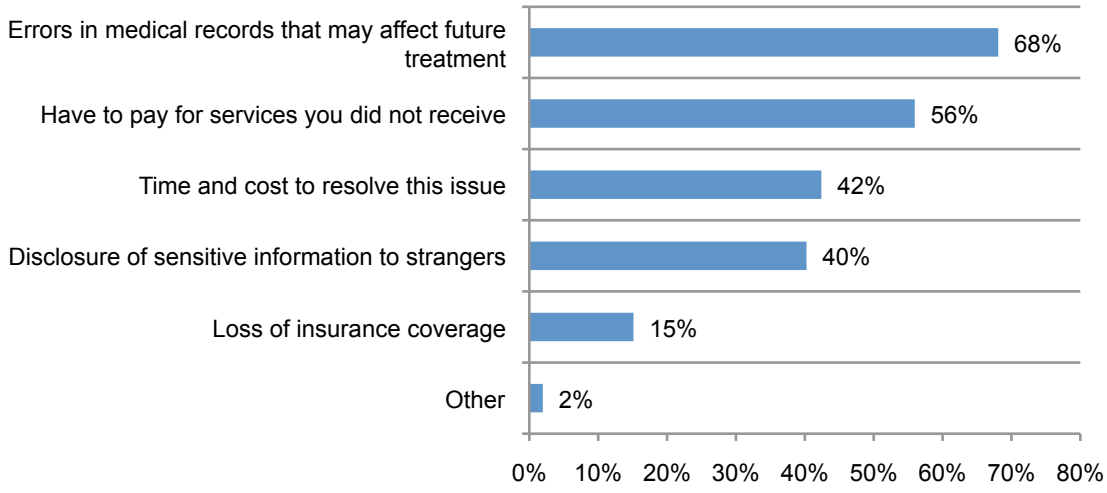
For purposes of this study, medical identity theft occurs when someone uses an individual's name and personal identity to fraudulently receive medical services, prescription drugs and/or goods, including attempts to commit fraudulent billings. This includes medical identity theft that occurs when an individual shares his or her credential with others. According to Figure 7, 59 percent of non-users and 51 percent of users say they are very concerned or concerned about becoming a medical identity theft victim as a result of insecure eHealth services or apps.

Figure 7. How concerned are you about becoming medical identity theft victim?
Very concerned and concerned responses combined



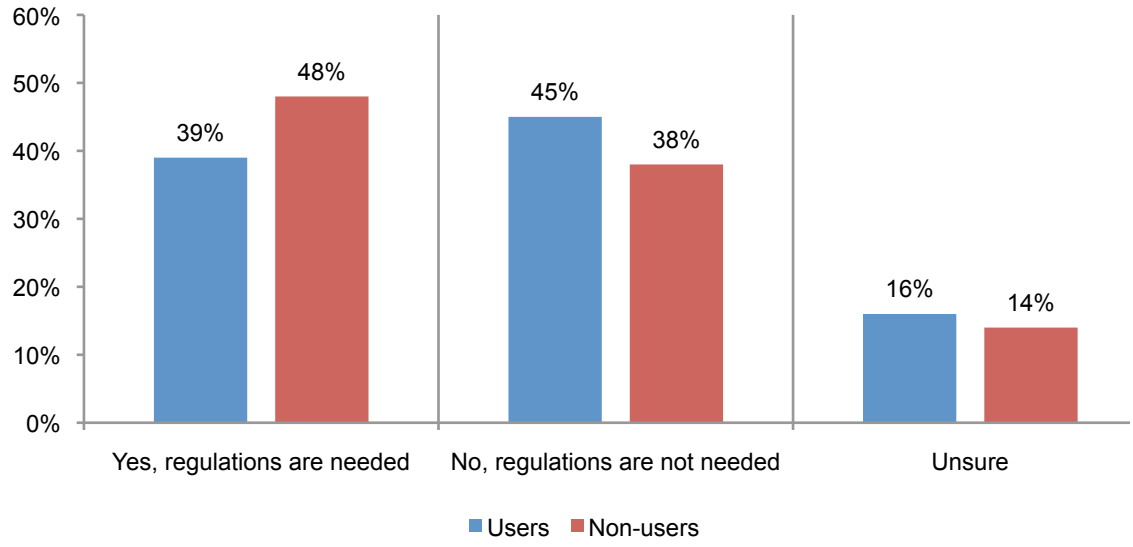
According to Figure 8, the two most worrisome consequences of medical identity theft are errors in medical records that may affect future treatment and the fees required to pay for services they did not receive. While not shown in the figure, non-users worry more about the disclosure of sensitive information to strangers (46 percent vs. 34 percent) and errors in medical records that may affect future treatment (70 percent vs. 66 percent).

Figure 8. Why respondents worry about medical identity theft
More than one response permitted



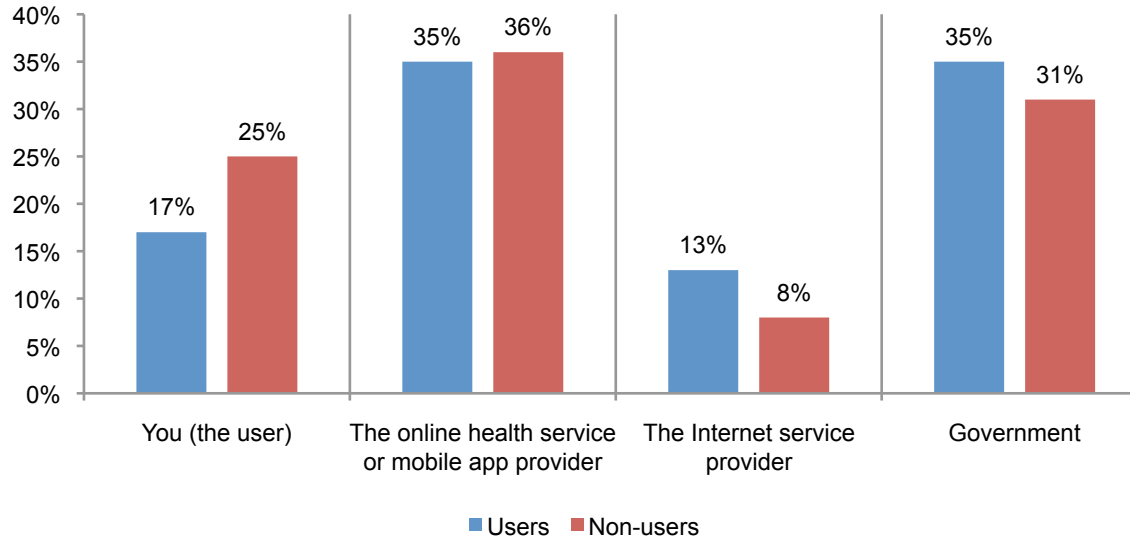
Are more regulations needed? Another significant difference between users and non-users involves the perception that government regulations are necessary to protect consumers' privacy rights when using eHealth services including mobile health apps. Figure 9 shows 48 percent of non-users believe increased regulatory protections are necessary as opposed to 39 percent of users (Diff = 9 percent).

Figure 9. Are more government regulations needed?
Strongly agree and agree response combined



Who should be responsible for privacy and security? When asked who should be most responsible for the security of their personal health information, 35 percent believe it should be government and another 35 percent say it should be the online health service or mobile app provider. Seventeen percent believe it is up to the individual and only 13 percent say it should be the Internet service provider, as shown in Figure 10. However, based on these results, 65 percent of users and 69 percent of non-users would want anyone but the government to be responsible.

Figure 10. Who is most responsible for protecting the privacy and security of eHealth users?



The age factor in eHealth

Age is a factor in how eHealth services are used. To determine differences in perceptions based on the age of the respondent, we analyzed the responses of those older than 35 years (53 percent of respondents) and those younger than 36 years (47 percent of respondents).

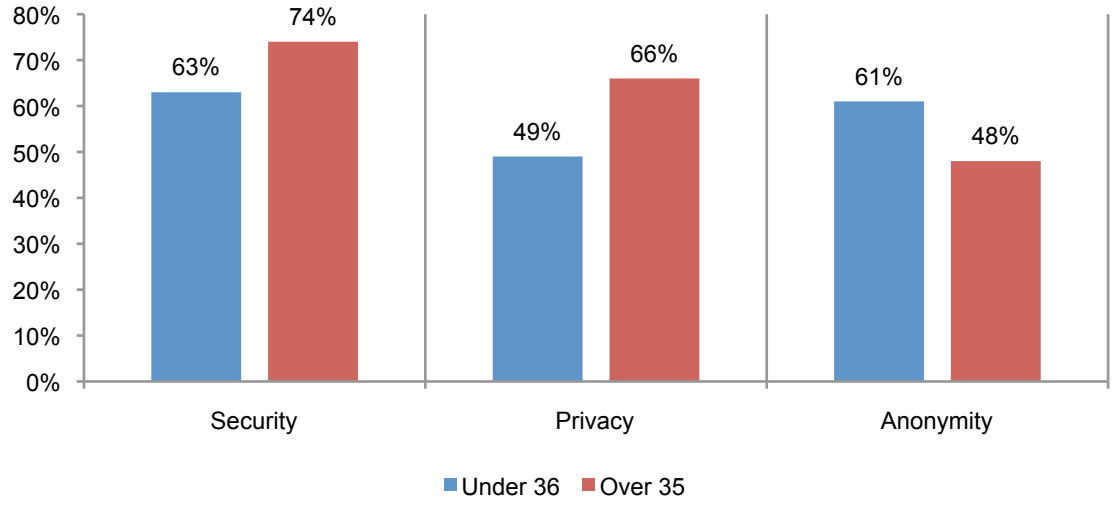
While most of the online health activities of these two groups are similar, it is interesting to note that older users are more likely to access and review their patient records and benefits statement. This is probably due to the likelihood that this age group will have more medical issues than those who are younger than 36 years old. Younger respondents also are more likely to substantially increase or increase their use of eHealth services over the next 12 months.

Another significant difference between the two groups is the notion of being anonymous when online. Fifty-four percent of younger respondents think that their privacy is protected when they can visit or search health websites without having to provide personal information. Forty percent of older respondents believe this to be true.

Anonymity is more important than privacy for younger users. As shown in Figure 11, 61 percent of respondents from the younger group believe anonymity is essential or very important in their decision to use online health services or mobile apps. Less than half of the older group (48 percent) believes this is critical.

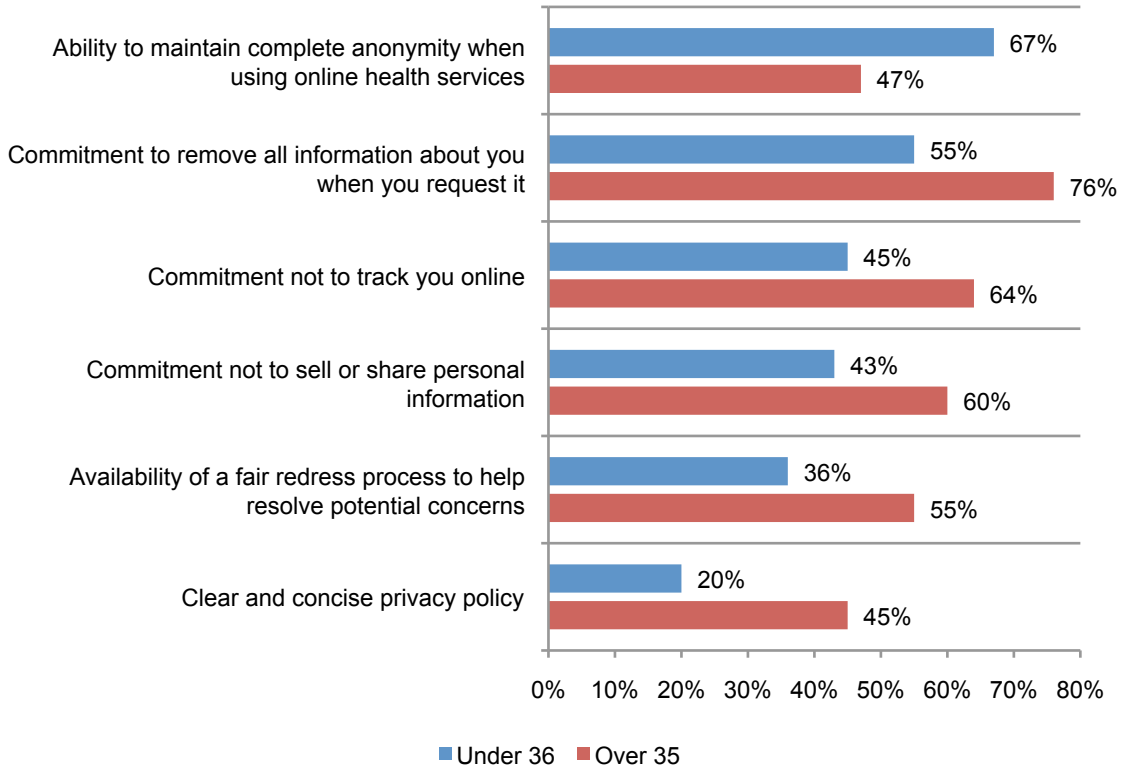
Figure 11 also shows the contrast in perceptions about the importance of privacy. Sixty-six percent of older users view privacy as essential or very important as opposed to 49 percent of younger users. Security is also more important for older users (74 percent vs. 63 percent).

Figure 11. Important factors when deciding to use online services
Essential and very important response combined



Older users are more concerned about privacy features. Figure 12 shows differences in perceptions about the importance of specific privacy features. Consistent with the other findings, younger users are most concerned about the ability to maintain complete anonymity while using online health services (67 percent vs. 47 percent). However, older respondents clearly view the other privacy features as critical with the exception of a clear and concise privacy policy.

Figure 12. What are the most important privacy features?
Essential and very important

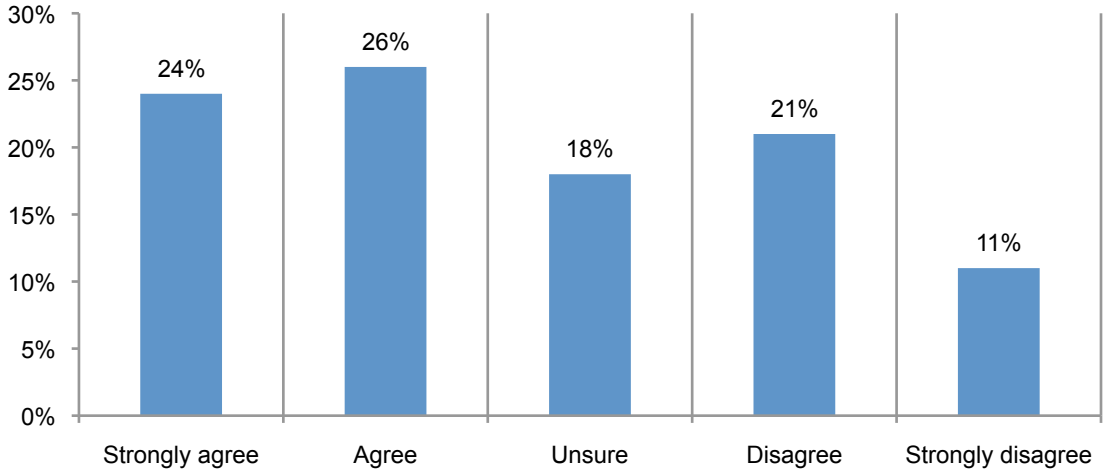


How to establish trust in eHealth services

The majority of respondents are not using eHealth services because of privacy and security concerns. A lack of confidence or trust in the protection of personal health information could be a major barrier to the successful implementation of online health services. Based on the findings, there are steps that can be taken to increase an individual's confidence and trust.

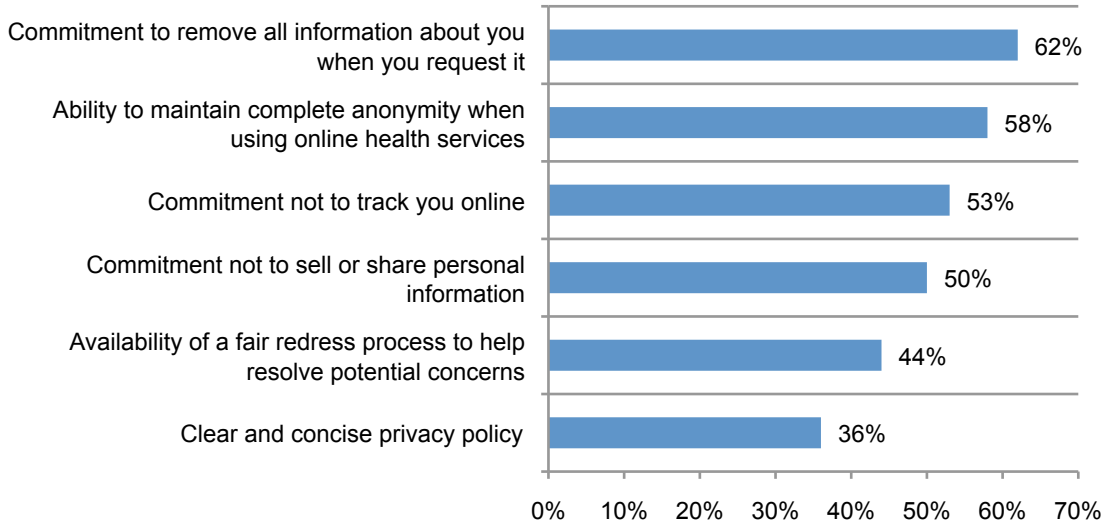
Limit the collection of personal health information. According to Figure 13, 50 percent of respondents believe their privacy is protected when they can search health websites without having to provide personal information. However, in those instances when personal information needs to be shared it should be limited and not extraneous to the service being provided.

Figure 13. My privacy is protected when I don't have to provide personal information



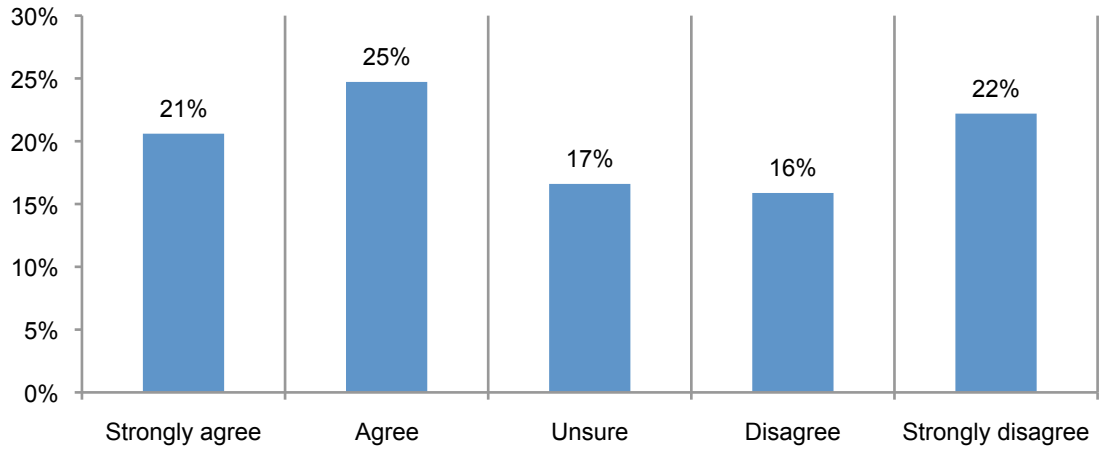
Respect the privacy preferences of consumers. According to Figure 14, the most important features are the commitment to remove all information about the consumer if he or she requests it followed by the ability to maintain complete anonymity when using online health services and the commitment not to be tracked online.

Figure 14. Important privacy features
Essential and very important



It is unclear that more government regulations would increase trust. Consistent with previous results (see Figure 9), 46 (21+25) percent of respondents strongly agree or agree with the proposition that regulations are necessary to protect their privacy rights when using online health services and mobile apps. Figure 14 shows 54 (22+16+17) percent of respondents strongly disagree, disagree or are unsure about the value of more regulatory oversight.

Figure 15. More government regulations are necessary to protect my privacy rights when using or accessing online health services and mobile apps.



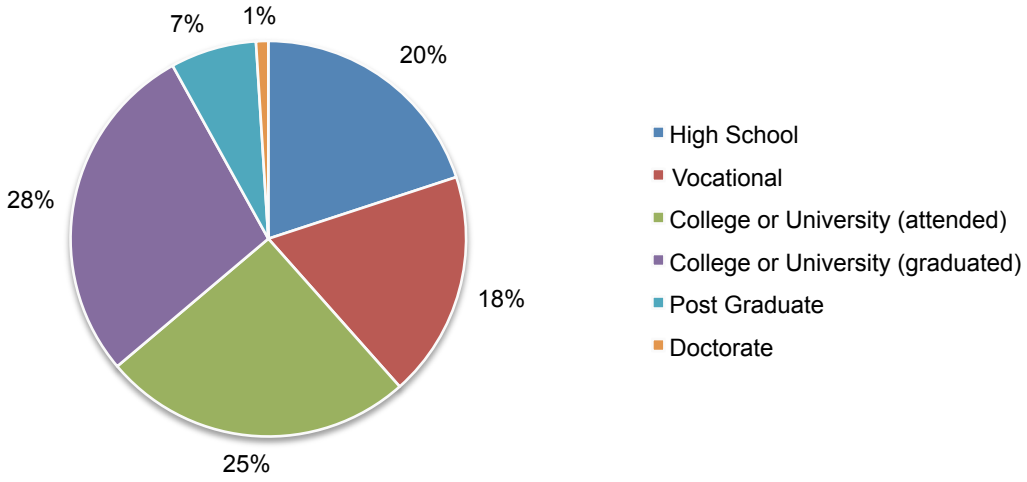
Part 4. Methods

A scientific consumer sampling frame of 25,755 adult-aged individuals who reside within the United States were selected as participants to this survey. As shown in Table 1,093 respondents completed the survey. After removing 124 surveys that failed reliability checks or screening criteria, we achieved a final sample of 969 qualified surveys, which represents a 3.8 percent response rate.

Table 1. Sample response	Freq	Pct%
Total sampling frame	25,755	100%
Total returns	1,093	4.2%
Screened or rejected surveys	124	0.5%
Final sample	969	3.8%

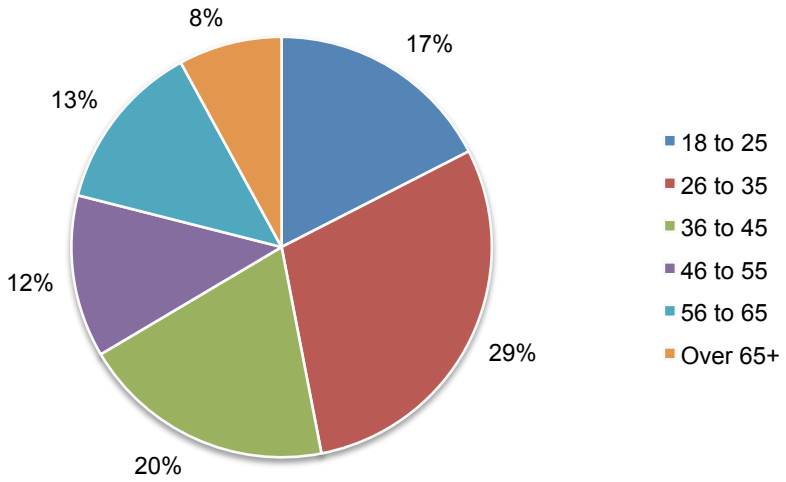
As shown in Pie Chart 1, the majority of respondents (53 percent) have attended college with 25 percent earning a degree.

Pie Chart 1. Educational background of respondents



Pie Chart 2 identifies 48 present of respondents are between the ages of 18 and 35.

Pie Chart 2. Age range of respondents



At 19 percent, the northeast and mid-Atlantic regions represent the largest segments. At 12 percent, the smallest regional segment is the southwest.

Pie Chart 3. Regional location of respondents

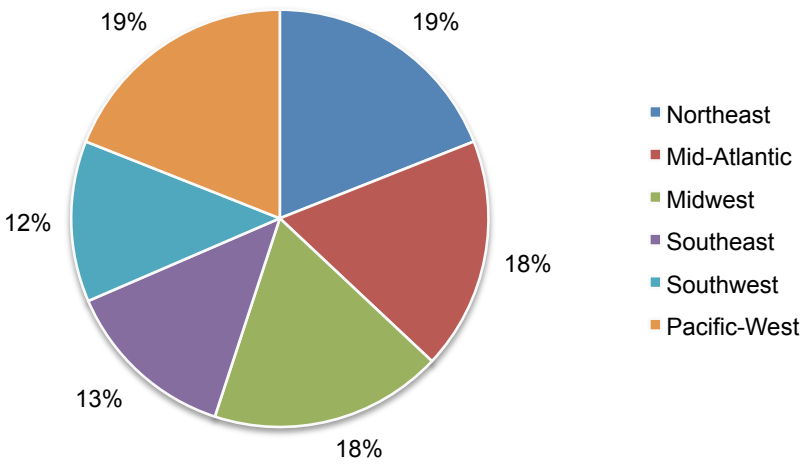
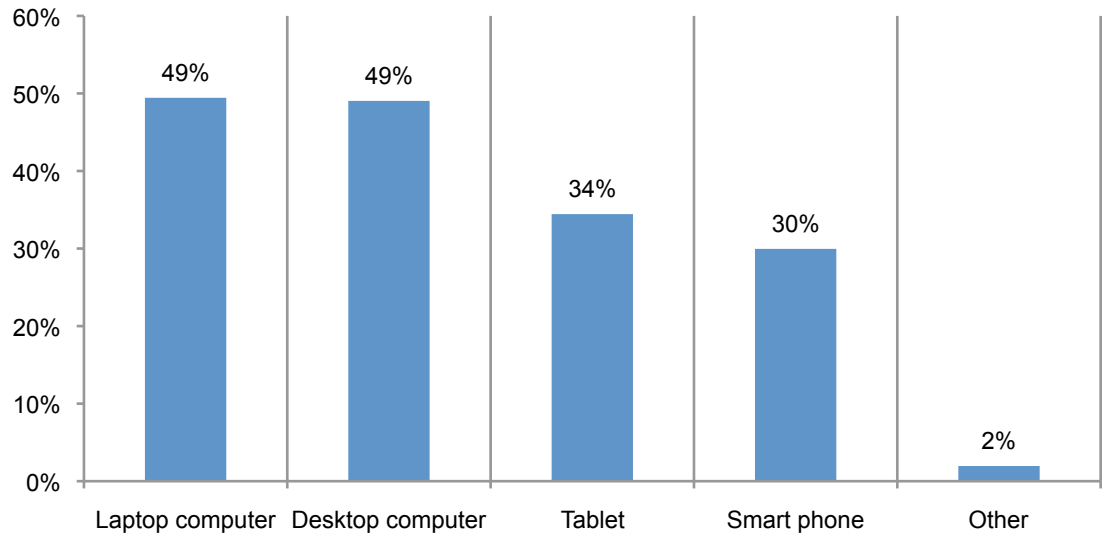


Figure 16 summarizes the types of computing devices that respondents in our study use to access the Internet. The two top choices are laptops and desktops at nearly 50 percent each.

Figure 16. Devices respondents use to connect to the Internet
More than one response permitted



Approximately 54 percent of respondents are female, 46 percent male. The percentage of respondents who claim to be single or head of household is 52 percent. Fifty-six percent of respondents are gainfully employees (full time, part time or business owner). Forty percent of respondents have a private health care plan, 32 percent have a public plan. See the Appendix to obtain additional sample demographics.

Caveats

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to many consumer-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of adult-aged consumers located in all regions of the United States, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.
- Sampling-frame bias: The accuracy is based on contact information and the degree to which the sample is representative of individuals who are likely to suffer from an identity theft crime. We also acknowledge that the results may be biased by external events such as media coverage at the time we fielded our survey.

  We also acknowledge bias caused by compensating respondents to complete this research within a holdout period. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.
- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that certain respondents did not provide accurate responses.

Appendix 1

The following tables summarize the percentage frequency responses to all survey questions. Please note that for certain questions, only users of eHealth services were asked to respondent. A total of 969 consumers completed the survey, of which 465 self-reported being users of eHealth services. The remaining 504 consumers were declared non-users of eHealth services.

Q1. What activities do you normally perform online or on mobile devices?	Overall
Emailing and texting	79%
Browsing and shopping	74%
Online searching & research	64%
Using social networks	49%
Sharing photos and videos	41%
Paying bills	26%
Blogging and using wikis	16%
None of the above	9%
Other	2%

Q2. Do you do any of the following health and wellness activities online? Please check all that apply.	Overall
None (splits same into user and non-user subsamples	52%
Browsing health-related Internet sites (such as WebMD)	33%
Monitoring and managing my weight	29%
Accessing and reviewing my patient records	28%
Performing searches on health-related topics	24%
Making payments to health care providers and/or insurer	23%
Monitoring and managing exercise program	20%
Diagnosing symptoms and possible medical conditions	19%
Receiving and reviewing explanation of benefits (EOB)	18%
Uploading and watching health-related videos	17%
Buying medications and medical devices	16%
Communicating (chatting) with my doctor or other clinicians	13%
Monitoring and managing vitals	12%
Communicating within health community through social media	11%

Q3. Do you believe your use of online health services will increase, stay the same or decrease over the next 12 months?	Users
Substantial increase	12%
Increase	23%
Stay the same	50%
Decrease	14%
Substantial decrease	1%
Total	100%

Q4. Which of the following health-related activities would you NOT perform online or through mobile apps because of privacy or data security concerns? Please check all that apply.	Overall
Accessing and reviewing my patient records	64%
Monitoring and managing my weight	58%
Performing searches on health-related topics	48%
Browsing health-related Internet sites (such as WebMD)	46%
Diagnosing symptoms and possible medical conditions	44%
None (no health-related activities are not performed)	39%
Making payments to health care providers and/or insurer	30%
Uploading and watching health-related videos	33%
Communicating within health community through social media	23%
Buying medications and medical devices	17%
Receiving and reviewing explanation of benefits (EOB)	21%
Monitoring and managing vitals	23%
Monitoring and managing exercise program	15%
Communicating (chatting) with your doctor or other clinicians	23%

Q5a. Does your doctor and/or health insurer encourage and/or incentivize you to use online health services and health-related mobile apps?	Overall
Yes	26%
No	74%
Total	100%

Q5b. If yes, what do you think about encouragement and incentives to use online health services and health-related mobile apps?	Users
I worry about the data security risks and choose not to use these services or apps	40%
I am aware of data security risks but still choose to participate	21%
I use them and do not have concerns about the security of my data	20%
I worry about the data security risks but the incentives outweigh my concerns	19%
Total	100%

Q6. How important is privacy in your decision to use (or not use) online health services or mobile apps.	Overall
Essential	28%
Very important	30%
Important	20%
Not Important	15%
Irrelevant	7%
Total	100%

Q7. How important is security in your decision to use (or not use) online health services or mobile apps.	Overall
Essential	38%
Very important	31%
Important	16%
Not important	11%
Irrelevant	5%
Total	100%

Q8. How important is anonymity in your decision to use (or not use) online health services or mobile apps.	Overall
Essential	27%
Very important	28%
Important	18%
Not important	16%
Irrelevant	11%
Total	100%

Q9. Are you aware of your rights under HIPAA as it relates to the privacy and data security of your online health information and records?	Overall
Yes	24%
No	76%
Total	100%

Q10. What online activities put your privacy and data security at greatest risk? Please choose your top three choices from the list below in terms risk level?	Overall
Accessing medical records	58%
Uploading videos and photos	39%
Making online purchases	37%
Using social networking	32%
Emailing and texting	33%
Researching using search engines (Google, Yahoo)	27%
Accessing health care benefit information	30%
Making payments	17%
Performing bank transactions	16%
Communicating with health provider	9%
Other	1%
Total	300%

Q11a. Have you or a close family member ever been notified by a health care provider or online health service that your personal information was lost or stolen as a result of a data breach?	Overall
Yes	35%
No	65%
Total	100%

Q11b. If yes, did you discontinue or terminate your relationship as a result of this data breach incident?	Overall
Yes	13%
No	87%
Total	100%

Q11c. If no, why not? Please choose one best choice.	Overall
Changing health providers is too difficult	49%
I wasn't harmed by the data breach	31%
I don't worry about privacy or security	9%
The health provider is not to blame	4%
I don't have a clear choice or alternative	6%
Other	0%
Total	100%

Q12. Should the US federal government (such as the USDA) regulate the privacy and data security of mobile applications used by doctors and hospitals?	Overall
Yes, regulations are needed	44%
No, regulations are not needed	41%
Unsure	15%
Total	100%

Q13a. How concerned are you about medical identity theft – such as the theft of your medical records, insurance credentials and more?	Overall
Yes, very concerned	23%
Yes, concerned	33%
Not concerned	45%
Total	100%

Q13b. If yes, why are you concerned? Please select all that apply.	Overall
Loss of insurance coverage	15%
Disclosure of sensitive information to strangers	40%
Errors in medical records that may affect future treatment	68%
Have to pay for services you did not receive	56%
Time and cost to resolve this issue	42%
Other	2%
Total	224%

Q14. Would you stop using your favorite social network provider such as Facebook or LinkedIn if they had a data breach involving your personal information?	Overall
Yes, with certainty	16%
Yes, very likely	25%
Yes, likely	30%
Not likely	29%
Total	100%

Q15. Would you stop using your favorite online health resource such as WebMD if they had a data breach involving your personal information?	Users
Yes, with certainty	24%
Yes, very likely	34%
Yes, likely	30%
Not likely	12%
Total	100%

Q16. Would you stop using your favorite mobile health app such as FITBIT if they had a data breach involving your personal information?	Users
Yes, with certainty	25%
Yes, very likely	36%
Yes, likely	22%
Not likely	17%
Total	100%

Q17. More government regulations are necessary to protect my privacy rights when using or accessing online health services and mobile apps.	Overall
Strongly agree	21%
Agree	25%
Unsure	17%
Disagree	16%
Strongly disagree	22%
Total	100%

Q18. I feel my privacy is protected when I can visit or search health websites without having to provide personal information.	Overall
Strongly agree	22%
Agree	25%
Unsure	19%
Disagree	26%
Strongly disagree	9%
Total	100%

Please rate the importance of each privacy feature listed below	
Q19a. Clear and concise privacy policy	Overall
Essential	8%
Very important	26%
Important	29%
Not important	29%
Irrelevant	9%
Total	100%

Q19b. Commitment not to track you online	Overall
Essential	22%
Very important	33%
Important	25%
Not important	13%
Irrelevant	7%
Total	100%

Q19c. Commitment not to sell or share your personal information	Overall
Essential	21%
Very important	31%
Important	21%
Not important	15%
Irrelevant	12%
Total	100%

Q19d. Commitment to remove all information about you when you request it	Overall
Essential	32%
Very important	34%
Important	11%
Not important	15%
Irrelevant	8%
Total	100%

Q19e. Ability to maintain complete anonymity when using online health services	Overall
Essential	26%
Very important	31%
Important	14%
Not important	20%
Irrelevant	10%
Total	100%

Q19f. Availability of a fair redress process to help resolve potential concerns	Overall
Essential	17%
Very important	29%
Important	22%
Not important	18%
Irrelevant	14%
Total	100%

Q20. In your opinion, who is most responsible for protecting the privacy and data security of your personal health information when using online health services or accessing mobile health apps?	Overall
You (the user)	21%
The online health service or mobile app provider	36%
The Internet service provider	10%
Government	33%
Total	100%

Part 3. Demographics

D1. Please check the devices you regularly use to use or access Internet services:	Overall
Laptop computer	49%
Desktop computer	49%
Tablet	34%
Smart phone	30%
Other	2%
Total	165%

D2. What is your present employment status?	Overall
Full time employee	41%
Part time employee	11%
Business owner	4%
Homemaker	12%
Retired	9%
Student	12%
Active military	2%
Unemployed	8%
Total	100%

D3. Approximately, when did you start using eHealth services?	Users
Within the past 2 years	35%
Between 3 to 5 years	43%
Between 6 to 10 years	15%
More than 10 years	7%
Total	100%

D4. What is your highest level of education attained?	Overall
High School	20%
Vocational	18%
College or University (attended)	25%
College or University (graduated)	28%
Post Graduate	7%
Doctorate	1%
Total	100%

D5. Please check your age range?	Overall
18 to 25	17%
26 to 35	29%
36 to 45	20%
46 to 55	12%
56 to 65	13%
Over 65+	8%
Total	100%

D6. What best describes your present health insurance or plan?	Overall
Private health plan	40%
Public health plan	32%
Medicare/Medicaid	13%
Veteran benefits (VA)	5%
Uninsured	11%
Total	100%

D7. Are you the head of household?	Overall
Yes	52%
No	48%
Total	100%

D8. Please check gender	Overall
Female	54%
Male	46%
Total	100%

D9. U.S. regional location	Overall
Northeast	19%
Mid-Atlantic	18%
Midwest	18%
Southeast	13%
Southwest	12%
Pacific-West	19%
Total	100%

For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org or calling our toll free line at 1.800.887.3118.

Ponemon Institute
Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**,we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.