

Ethics Survey of Consumer Attitudes About Health Web Sites

SPONSORED BY

California HealthCare Foundation and
Internet Healthcare Coalition

CONDUCTED BY CYBER DIALOGUE

Thaddeus Grimes-Gruczka and
Carolyn Gratzer in cooperation with
The Institute for the Future

2nd Edition September 2000
Originally released January 2000

ISBN 1-929008-38-4

ACKNOWLEDGMENTS

Institute for the Future

The survey instrument was developed under the direction of the Institute for the Future, a nonprofit research and consulting firm dedicated to understanding technological, environmental, and societal changes and their long-term consequences. IFTF can be found on the Web at www.iftf.org.

We would like to acknowledge the participation of individuals whose expertise was invaluable to that process: Mary Cain, Director, Institute for the Future; Janlori Goldman, JD, Director, Health Privacy Project at Georgetown University; Zoe Hudson, Senior Policy Analyst, Health Privacy Project at Georgetown University; Sam Karp, Chief Information Officer, California HealthCare Foundation; Robert Mittman, Director, Institute for the Future; Jane Sarasohn-Kahn, Research Affiliate, Institute for the Future; Denise Silber, Internet Healthcare Coalition; and Jennifer Wayne-Doppke, Research Affiliate, Institute for the Future.

Cyber Dialogue

We also would like to thank these individuals at Cyber Dialogue who were instrumental in the conduct and analysis of this research: Joe L. Farris II, Account Executive; Kevin Mabley, Director of Research; Thomas E. Miller, Vice President; Julie Anne Rodriguez, Analyst; David Stein, Publisher; Luis Torroella, Associate Director; and Cathlin Tully, Analyst.

Internet Healthcare Coalition

The Internet Healthcare Coalition is a nonprofit, nonpartisan organization dedicated to identifying and promoting quality healthcare resources on the Internet. IHC's goal is to help healthcare consumers and professionals stay informed about the evolving issues relating to the quality of Internet health resources and information. IHC can be found on the Web at www.ihealthcoalition.org.

Additional copies of this report can be obtained by calling the California HealthCare Foundation's publications line at (510) 587-3199. The report is also available as a PDF at ehealth.chcf.org.

Contents

EXECUTIVE SUMMARY	4
METHODOLOGY	5
INTRODUCTION	6
FINDINGS	7
I. GENERAL CONCERNS ABOUT PRIVACY PERMEATE SOCIETY AND THE INTERNET COMPOUNDS MANY OF THOSE FEARS	7
II. HALF OF INTERNET USERS CONCERNED ABOUT POTENTIAL FOR INVASION OF PRIVACY OF PERSONAL HEALTH INFORMATION	8
III. BALANCING PRIVACY AND PERSONALIZATION	9
IV. TRACKING WITH COOKIES: THE NEED FOR CONTINUING EDUCATION	11
V. HEALTH NON-SEEKERS: BARRIERS AND OPPORTUNITIES	12
VI. INFLUENCE OF SITE SPONSORSHIP AND E-COMMERCE ON INFORMATION SHARING	12
VII. DIVERGENT OPINIONS ABOUT SPECIFIC ONLINE OFFERINGS	14
VIII. DRIVERS OF INCREASED TRUST AND POSITIVE OPINION CHANGE	16
IX. WHO IS MINDING THE STORE? WHO SHOULD?	18
CONCLUSION	20

Executive Summary

The *Ethics Survey of Consumer Attitudes About Health Web Sites* demonstrates that the average U.S. Internet user is:

- concerned about the privacy of online health information;
 - suspicious of the ethics of many health Web sites;
 - uncertain whether personal health data are protected by law; and
 - confused about who should regulate Internet health information, or if it should be regulated at all.
1. Internet users overwhelmingly do not want their health information shared with anyone else without their consent. Eighty-eight percent of respondents said they would not be willing to submit information if it were to be shared with advertisers or marketers. In fact, they are more concerned about a site sharing information with advertisers than they are about someone hacking into the site and gaining access to their information. There is also a high level of concern about access to personal health information by insurers and employers who might use that information against them.
 2. Online medical record keeping, even if access is restricted to an individual and his or her physician, is perceived as the greatest threat to individual privacy on the Internet. These numbers are particularly significant, given that these are some of the major services that healthcare companies are trying to expand online.
 3. Physicians may hold the key to overcoming consumers' fears. Internet health consumers are most likely to trust their physicians, medical institutes, and associations to maintain the privacy of their personal health information. They trust pharmaceutical companies, Web portals, and online drugstores the least. Consumers are more willing to provide information to (and trust the content of) a site that has been recommended by their doctor, or if there is a privacy statement on the site stating that information will not be shared. Paradoxically, while 78 percent of respondents say a privacy statement on a site is a positive influence on their likelihood to use that site, fully two-thirds of all respondents say they "sometimes, rarely, or never" read those privacy statements, nor do they check to see who sponsors the sites that they're using. These data indicate that meaningful privacy policies can have a positive impact on willingness to engage in online health activities. But despite their concern, the majority of Internet users have not yet taken an active role in educating themselves about online security issues.
 4. People don't know if their privacy is legally protected (a fact mirrored by polls showing most people believe there is a federal law that protects medical records). Further, Internet users are sharply divided over who, if anyone, bears responsibility for regulating health information and services on the Internet.

5. Seventeen percent of Internet users will not even search for health information online because of privacy concerns. Despite the real risks to privacy posed by the Internet, this statistic hints at a level of concern that may be unwarranted—simply searching for information, without registering or providing other personal information, could be an anonymous activity. This fear may be an impediment to the adoption of services that may provide significant benefits to consumers in the future.

METHODOLOGY

The California HealthCare Foundation commissioned Cyber Dialogue to conduct a survey to measure U.S. online adults' concerns regarding the ethical conduct of healthcare Web sites and services on the Internet. To meet this objective, Cyber Dialogue surveyed via the Internet a nationally representative sample of 1,009 U.S. online adults age 18 or older. The survey was conducted January 10-17, 2000. All respondents are members of Cyber Dialogue's database of online users. Quotas were established to interview 750 respondents who currently seek health and medical information online and 250 who do not. Respondents were sampled and weighted, based on Cyber Dialogue's *American Internet User Survey (AIUS)*, to reflect nationally known norms for online adults in terms of age, gender, household income, ethnicity, health status, Internet tenure, and whether they use the Internet for health and medical information.

SECOND EDITION

To further explore the attitudes of minority groups on privacy and online healthcare, Cyber Dialogue fielded the survey a second time from February 22-March 6, 2000. In each of four minority groups—low household income (less than \$25,000 annually), Asian, African American and Hispanic—approximately 200 individuals from Cyber Dialogue's database of online users were surveyed, at least 100 of whom seek online health information. The data from each minority group were weighted, based on Cyber Dialogue's AIUS, to reflect nationally known norms for online adults in that group in terms of age, gender, household income, health status, and whether they use the Internet for health and medical information.

Introduction

HEALTH. PRIVACY. TECHNOLOGY. Each topic on its own has played a central role on the national stage for decades, and each maintains its prominence at the start of the new millennium. With the advent of wider access to the Internet, and the growing promise (or, as portions of this report may indicate, the growing threat) that the convergence of healthcare information, personal information, and Internet-based collection and distribution of both has wrought, the issue of personal privacy as it relates to health matters has never been more important.

As of the end of 1999, some 34.7 million adults in the United States, or 48 percent of all those online, were using the Internet to collect health information—making health and medicine the fourth-most-popular content type online behind news, travel, and weather. The number of online health users continues to grow at twice the rate of the overall online population in the United States and will reach 88.5 million by 2005. Among online adults, Caucasian Americans are significantly more likely to seek health information (49 percent of Caucasian online adults do so) than are African Americans (38 percent), Asian Americans (37 percent), and Hispanics (29 percent). Already, almost 7 million U.S. adults are purchasing health and beauty products online, and almost 3 million are connecting with providers and payers online. Our conservative forecasts suggest that by 2005, more than 40 million U.S. adults will use the Internet for health commerce, and more than 50 million will connect with healthcare professionals online. With the growth of health e-commerce and connectivity, both of which require consumers to share personal health and financial information online, privacy issues surrounding healthcare on the Internet will become increasingly urgent and complex.

The dramatic revolution that has resulted from the array of healthcare-related consumer, connectivity, and e-commerce Web sites poses a series of complicated ethical and legal questions—most of which bewilder the consumer, few of which have been addressed adequately by the institutions upon which the consumer depends for security. The data reported here, collected from in-depth interviews of more than 1,000 Internet users in the United States, point to the urgent need for a thoughtful, thorough, and fair discussion of ways to secure individual privacy, foster strong ethical behavior, and harness the incredible power of the Internet to improve the quality of healthcare for all Americans. By necessity, this discussion must include all concerned parties: traditional healthcare organizations (insurance companies, pharmaceutical manufacturers, hospitals, etc.), Internet health players, appropriate regulatory organizations, and, most important, the individual consumer. The California HealthCare Foundation and the Internet Healthcare Coalition have sponsored this groundbreaking study with the intention that it will spur such a discussion at the national level.

Findings

I. GENERAL CONCERNS ABOUT PRIVACY PERMEATE SOCIETY AND THE INTERNET COMPOUNDS MANY OF THOSE FEARS

Americans using the Internet are concerned about protection of their privacy not only while online but in their everyday lives and activities. When asked to answer “How concerned are you about the potential for invasion of your personal privacy in the U.S. today?” on a scale from 1 (“not at all concerned”) to 5 (“very concerned”), fully 61 percent of all respondents placed their level of concern at 4 or 5. Among seekers of health information on the Internet (“health seekers”), that figure rose to 66 percent.

Among populations that may perceive themselves as more vulnerable to breach of privacy—online health information seekers over 50, online health information seekers with household incomes under \$50,000 per year, and online health information seekers of color—the ratio rose to 72 percent, 71 percent, and 72 percent for each group, respectively. Asian Americans, in particular, show a high level of concern about privacy, with 74 percent concerned or very concerned.

These data show that the ongoing American debate about the scope and sanctity of our perceived right to privacy has extended into the Internet sphere. For example, Figure 1 also shows the majority of respondents—52 percent—are even more concerned about general invasion of privacy occurring on the Internet than by other means, with 49 percent of health seekers sharing that measure of concern. Among Hispanic Americans, this incidence rises to 63 percent (58 percent for health seekers); and among Asian Americans, it increases to a substantial 72 percent (70 percent for health seekers). These numbers indicate unease about privacy even among individuals already comfortable using the Internet to access information and services for themselves and their families.

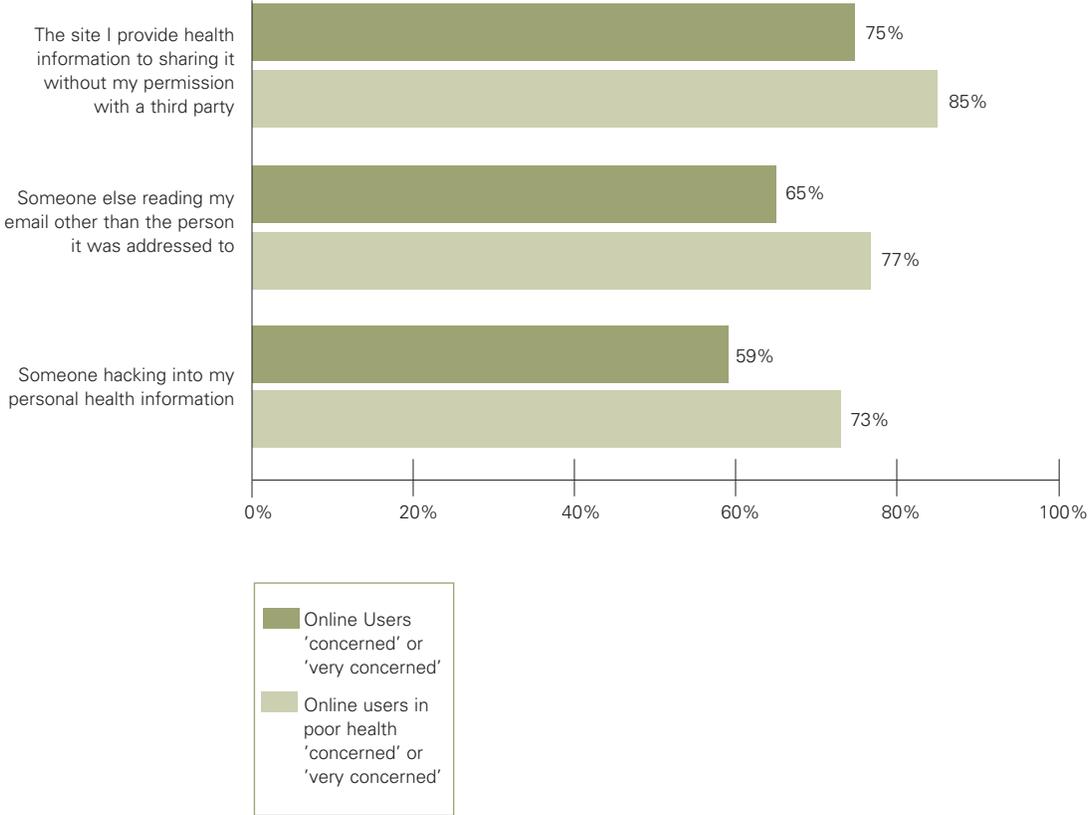
Figure 1: Concern regarding personal privacy on Internet vs. personal privacy in general.

	ONLINE ADULTS	HEALTH SEEKERS	NON-SEEKERS
Concerned/Very Concerned about personal privacy in general	61%	66%	59%
More concerned about Internet	52%	49%	53%
Less concerned about Internet	8%	12%	6%
Neither more nor less concerned	40%	39%	41%

II. HALF OF INTERNET USERS CONCERNED ABOUT POTENTIAL FOR INVASION OF PRIVACY OF PERSONAL HEALTH INFORMATION

When asked specifically about preserving the privacy of health information in the United States (whether online or offline), the survey found similar rates of concern. When questioned about particular types of breaches of privacy, the vast majority of respondents rated themselves “concerned” or “very concerned” about the following three issues. Not surprisingly, those in poor or fair health are more concerned than average about breaches of privacy, especially by employers and insurance companies who they fear could use this information to discriminate.

Figure 2: Three main health privacy issues concern online users.

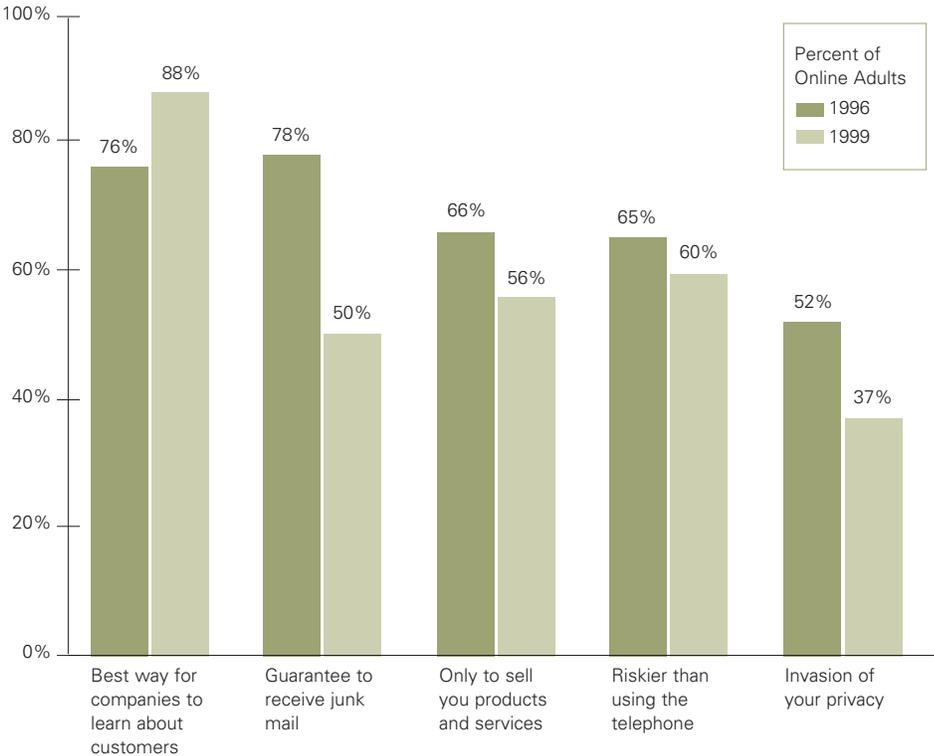


III. BALANCING PRIVACY AND PERSONALIZATION

This survey confirms the findings of earlier privacy studies conducted by Cyber Dialogue that have shown there is a range of personal information that individuals are willing to share with Internet sites, provided that information is:

- used to enhance the quality of their online experience, and
- not subject to unwarranted or undisclosed sharing or abuse.

Figure 3: Submitting personal information online is . . .



Comfort levels with revealing certain types of personal data as part of a site’s registration process have grown as the Internet is used more widely. But, as Figure 4 shows, disclosing personal health information still raises concerns, with just 18 percent of all respondents willing to do so in return for a more personalized Web service. This figure compares with acceptance rates for disclosing email addresses, name, and gender, all of which reach well into the 80+ percent range. A person’s favorite color (a fact sometimes used by Internet marketers to personalize banner advertisements to make

them more attractive to individual users) is disclosed willingly by 72 percent of users, address by 55 percent, and ethnicity by 61 percent overall. Among ethnic minorities, an interesting split emerges: While Hispanic-American health seekers are just as likely as the average to disclose their ethnicity, Asian Americans (55 percent) and African Americans (56 percent) are less likely to do so.

Figure 4: Users willing to provide sites with personal information for more customized service, but don't want that information shared with third parties.

	USERS WILLING TO PROVIDE THIS INFO TO SITE FOR MORE PERSONALIZED SERVICE	USERS OK WITH WEBSITES SHARING THIS INFO WITH OTHER SITES, COMPANIES, AND ADVERTISERS
Email address	90%	18%
Gender	87%	27%
Name	82%	15%
Favorite color	72%	22%
Ethnicity	61%	18%
Address	55%	8%
Employer	21%	2%
Health information	18%	3%
Credit card number	11%	0%
Promotions you respond to	50%	31%
What ads you click on	28%	48%
Products you buy on the site	26%	55%

Only credit card information is more closely guarded than health data: 10.5 percent of all respondents are willing to disclose their credit card numbers in exchange for personalized Web site service. This finding is consistent with previous Cyber Dialogue research from 1999, which found a similarly higher level of vigilance regarding credit card numbers as compared to other personal information.

Figure 5: Internet users are protective of their credit card information.

	"THE INTERNET POSES A RISK TO MY PRIVACY."	"THE INTERNET POSES A RISK TO MY CREDIT CARD NUMBER."
Strongly Agree	9%	30%
Agree	33%	38%

Source: Cyber Dialogue, 1999

When the survey considered less sensitive information (such as products purchased online, or promotions to which a consumer responded), a majority of those surveyed were comfortable having these types of data points collected without their explicit consent. Opinion changes drastically, however, when users are asked whether it is acceptable for information gathered during the site registration process to be shared with other Web sites, companies, or advertisers. For example, looking again at Figure 4, while 90 percent of those surveyed were willing to give their email address to a site, only 18 percent of respondents said it was acceptable for the site to share that information. Eighteen percent were willing to share health information to register, but just 3 percent were comfortable with those data being shared with a third party. Even the gap in willingness to share one's ethnicity closes in this context; health seekers overall, only 17 percent of whom would share ethnicity information with a third party, are no more likely to do so than the ethnic minority groups surveyed.

IV. TRACKING WITH COOKIES: THE NEED FOR CONTINUING EDUCATION

Interestingly, the tracking technology referred to as "cookies" (which places an electronic tag on an individual's Internet browser and tracks Web site visits) is well known, at least in the broadest of senses; and the technology is seemingly well accepted by the vast majority of Internet users. Eighty-four percent of all Internet users (and 89 percent of health seekers) are aware of cookies, but only 4 percent of users set their browsers to reject all cookies automatically. (Among African Americans, awareness of cookies drops to 77 percent, and only 2 percent automatically reject them.) On the other hand, there is some confusion in the minds of consumers as to exactly what purpose cookies serve. Twenty-one percent of health seekers feel that a site should not collect any information whatsoever about a visit without gaining the user's explicit permission—this includes pages visited, ads clicked on or products bought on that site. That leaves at least 6 percent of health seekers who keep cookies enabled but oppose the automatic collection of information, signaling a need for further consumer education on the issue. Particularly in the wake of the negative press surrounding DoubleClick's information collection

Good Cookies: Meet Me, Remember Me, Value Me

A company can use cookies on a site for many valid reasons: security, personalization, marketing, customer service, etcetera. Try surfing the Web with your browser set to reject cookies and see how cumbersome even the easiest of online tasks becomes. Most important, cookies are legitimate tools in understanding how someone uses a particular site to improve his or her experience. Banning all cookies is the equivalent of telling supermarkets that they can't organize their aisles based on the behavior of people in the store or that a storekeeper can't greet a repeat visitor because he or she remembers the customer on a repeat visit. In other words, the early developers of the technology intended cookies to be used as a way to minimize navigational inconveniences and maximize personalization spurred, organically, by online consumer behavior. Individual sites or families of sites still use cookies successfully and ethically in this way.

Bad Cookies: Tracking Across Sites Through Banner Ad Networks

Here is a little-known fact about banner ads: They, too, utilize cookies. When a user clicks on a link in a banner ad served by an online advertising network, the click first goes back to the ad network company to make a record of the clicked link. Only then does the ad network's server redirect the user's browser to the advertiser's Web site. An ad network cookie, sometimes referred to as a third-party cookie, belongs to the ad network and operates independently of the host Web site cookie. It operates like a standard cookie, except that data collected by the ad network cookie is sent back to the ad network instead of to the host Web site. These third-party cookies allow an ad network to profile users just as a host Web site cookie does.

But there is an important, if widely ignored, distinction between the use of cookie tracking on a single company's sites versus tracking across unrelated sites. Ad-serving companies are able to connect unrelated sites and overcome the site-specific nature for which cookies were originally designed. Some ad-serving companies are now connecting this aggregated data with offline demographic and credit card data as well. It is this "connecting of the dots" behind the scenes that can become dangerously invasive. For example, it is possible for a banner ad company to match an article someone is reading on one Web site with a health condition that the person is researching at another health site. What further raises the hackles of privacy advocates is that these cookie profiles are then sometimes linked with third-party consumer databases that contain name, address, date of birth, and more. Reselling disparate data sources connected to form a thorough profile of an individual has the potential to demolish the sanctity of that consumer's personal information.

Sources: California HealthCare Foundation, *Report on the Privacy Policies and Practices of Health Web Sites*, January 2000; and Kevin Mabley, *Privacy vs. Personalization, Part III*, Cyber Dialogue, 2000.

practices, which occurred after the first wave of this survey was fielded, consumers will need continuing education on how to separate the appropriate from the inappropriate uses of tracking technologies. The two sidebars should be useful in educating your consumers and partners alike on the truths behind tracking for cookies and banner ads.

V. HEALTH NON-SEEKERS: BARRIERS AND OPPORTUNITIES

Approximately 37 million U.S. Internet users are not currently using online health information. One-third of health non-seekers cite that they have no need for online healthcare information, either because they consider themselves healthy or simply due to a lack of interest. Privacy and security concerns, cited by 17 percent of non-seekers, represent the greatest barriers to online health usage by otherwise interested individuals: 12 percent attribute their non-seeker status to privacy concerns and 8 percent to security worries. Notably, these percentages differ significantly for the minority groups. Only 6 percent of Hispanic Americans, 7 percent of African Americans, 9 percent of those making less than \$25,000 annually, and 12 percent of Asians attribute their non-seeker status to privacy or security concerns. These groups are more likely than average to prefer information from other sources (often, from their doctors) and to cite a lack of need for online health information. Targeting potential customers who are members of minority groups represents an important element of a successful acquisition strategy.

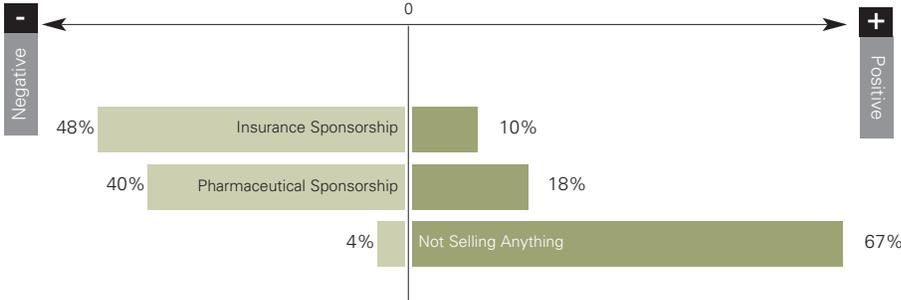
Non-seekers in general demonstrate high levels of interest in a variety of online health applications, from personalized disease sites (71 percent) to e-mail communication with their doctors (45 percent) to the purchase of prescription drugs (24 percent)—all of which require the submission of personal information. A real opportunity exists to create the gold standards of privacy and security in online healthcare and to educate consumers on the truths behind these issues. Current non-seekers will flock to sites that can promise them a secure, private online experience.

VI. INFLUENCE OF SITE SPONSORSHIP AND E-COMMERCE ON INFORMATION SHARING

With so many online business models incorporating editorial content, advertising, or commercial sponsorship and e-commerce, the question of how best to ethically combine these somewhat conflicting elements into one site weighs heavily upon the minds of many e-healthcare executives. Our data show that this issue also concerns consumers and affects their willingness to share personal information with a site. Forty-eight percent of health seekers state that knowing

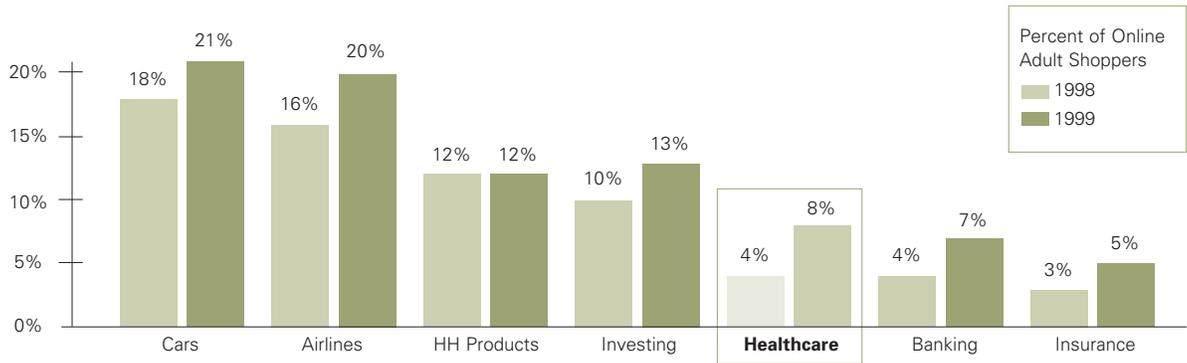
a site is sponsored by an insurance company would negatively impact upon their choice to submit personal information to that site, while only 10 percent cite insurance sponsorship as a positive influence. Similarly, pharmaceutical company sponsorship would cause 40 percent of health seekers to think twice before sharing personal information online and would encourage only 18 percent to do so. (Asian-American and African-American health seekers are slightly less likely to be deterred by pharmaceutical and insurance company sponsorship.) Conversely, noting that a site is not trying to sell anything would positively influence information sharing for 67 percent of health seekers and deter sharing for only 4 percent.

Figure 6: Effects of sponsorship and e-commerce on information sharing.



Clearly, insurance and pharmaceutical companies will need to fight an uphill battle to gain trust; consumers will require proof that these companies will respect the integrity of their personal information. However, Cybercitizen Health data show that the online experience has changed the brand opinions of more than 40 percent of consumers in seven major categories. In healthcare alone, 8 percent of consumers report having changed their opinion of a brand because of the Internet—a 100 percent gain year-over-year. By leveraging the specific suggestions in the next few sections, pharmaceutical companies, insurance companies, and others can build consumer trust and loyalty. On the e-commerce front, our data reinforce the already clear need for all health sites to separate editorial content from merchandise and advertising. While we believe that the convenience of total disease and wellness management online will ultimately outweigh consumer privacy and security concerns, it is imperative that all health sites incorporating both commerce and content take decisive steps to prove to consumers that they are handling this issue ethically.

Figure 7: Brand impacts of the Internet are growing.



VII. DIVERGENT OPINIONS ABOUT SPECIFIC ONLINE OFFERINGS

The Internet has the potential to provide a multitude of services to the healthcare consumer, from the timesaving (online health insurance claims processing) to the lifesaving (access to vital health information from any emergency room around the world). When Internet users were asked about this range of possibilities, as well as the desirability and the potential risks of each, they responded with the most divergent opinions found in this survey.

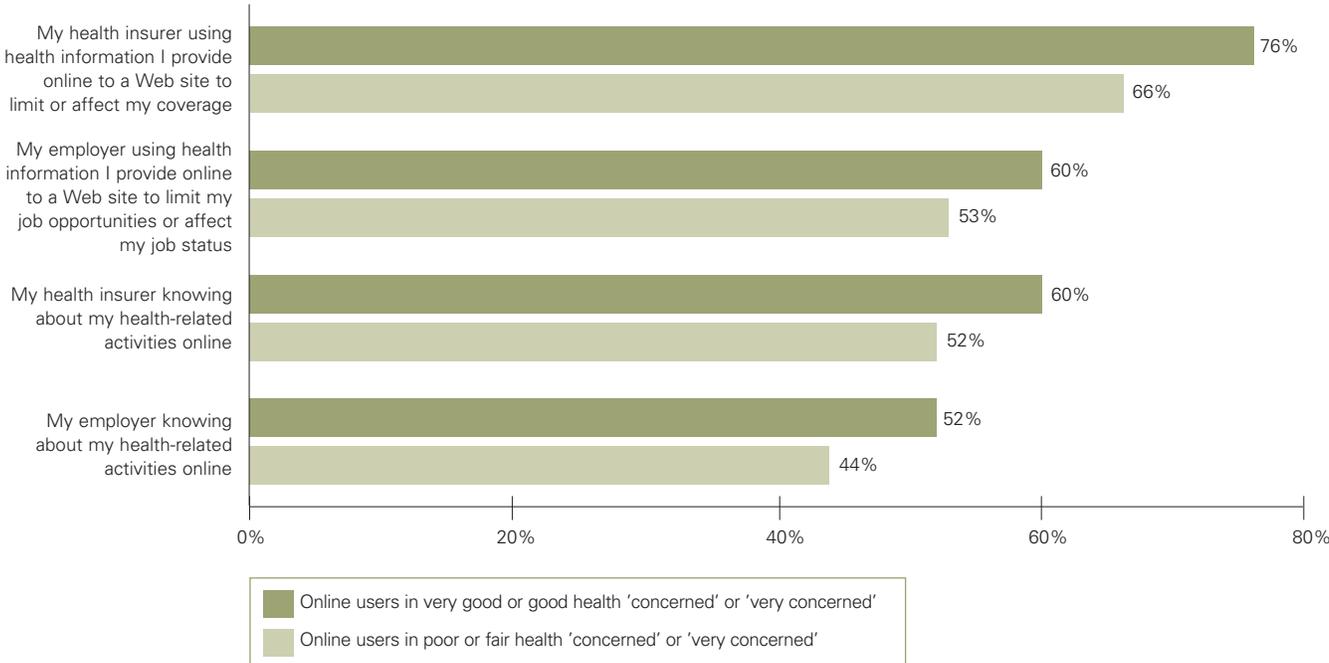
Figure 8: “Indicate your level of privacy/confidentiality concerns for each of the following healthcare-related online activities.”

TYPE OF ACTIVITY	WOULD DO	WOULD NOT DO BECAUSE OF CONCERN
Allow my doctors to have access to my personal medical record online	42%	40%
Access my personal medical record online	38 %	40%
Have password-protected Internet access to my medical record in my doctor’s office	47%	33%
Sign up for or purchase health insurance online	37%	27%
Personalize a health information site by selecting information to have updated whenever I visit the site	37%	26%
Purchase or refill prescription drugs online	45%	25%
Seek advice online regarding a specific medical condition from other online patients	51%	18%
Use a secure Web site	48%	17%
Register at a health-related Web site	43%	16%
Participate in a health-related chat room	36%	15%
Purchase a health product other than a prescription	53%	12%
Access the latest disease-specific research or news	56%	3%

In short, the very aspects of Internet-driven healthcare that hold the most promise for improving care delivery are the same aspects that raise the most concern among the public. Online medical record keeping, even if access is restricted to an individual and his or her physician, is perceived as the greatest threat to individual privacy, a fact that will resonate among the many Internet healthcare players planning to offer such services.

Online health seekers are also concerned that insurers could use private personal health data to limit or affect their insurance coverage, or that employers could use such information to limit job opportunities. In fact, many Internet users fear that the mere act of searching for general health-related information online may bring repercussions from insurers and employers. Across the board, individuals in poor or fair health are more likely to report that they would stay away from online healthcare activities due to privacy concerns—at least in part because of the greater potential for abuse of their personal health data by employers and insurers.

Figure 9: Concerns about employer and insurance company access to personal health information.



VIII. DRIVERS OF INCREASED TRUST AND POSITIVE OPINION CHANGE

Online users' fears about making personal health information available on the Internet can be assuaged, however. The survey found several measures that, if implemented, could have a distinctly positive impact on users' inclination to release personal health information online. They include physician recommendation; published privacy statements pledging not to share information with advertisers, marketers, and other sites; and individual control over the distribution of information.

Figure 10: Positive drivers of willingness to submit information online.

	ALL ONLINE USERS
Site is recommended by your doctor	80%
Site has published a privacy policy statement that claims information you submit will not be shared with advertisers	79%
Site gives you the opportunity to see who has access to your profile	78%
Site allows you to make choices about the use of your information	78%
Site has published a privacy policy that claims information you submit will not be shared with other sites or marketing partners	78%

(These factors are, not surprisingly, similar to those that influence a person's likelihood to trust any given site's content. Research conducted by Cyber Dialogue in 1999 found that a doctor's recommendation of a particular health site's content led 74 percent of online health users to trust the information they found there.)

Conversely, a number of variables can negatively influence consumers' willingness to share personal information; most significantly, linkages that share information with a site's advertisers and marketing partners.

Figure 11: Negative influencers of willingness to share health information online.

ALL ONLINE USERS	
Site shares your profile with its advertiser or marketing partners	88%
Site automatically collects information about you	79%
Site is sponsored by an insurance company	45%
Site is sponsored by a pharmaceutical company	40%
Site was promoted by national TV ad or television program	19%

Finally, several factors, including seals of approval from Internet trade groups such as HON and TRUSTe; sponsorship by nonprofit organizations; and the presence of banner advertisements, have no impact—positive or negative—among the majority of respondents. The lack of influence of seemingly disparate factors may point to an increasingly sophisticated ability among online users to discern fact from hype.

Figure 12: Characteristics with no impact on willingness to submit health information online.

ALL ONLINE USERS	
Site has seal of approval from trade groups such as HON or TRUSTe	53%
Site is sponsored by a nonprofit organization	52%
Site is sponsored by patient groups	50%
Site is free of banner advertisements	50%
Site is sponsored by a library or medical librarians	49%

One fact is perfectly clear: Internet users respond favorably to clear, meaningful policies that protect the privacy of personal information. Privacy policies, with proper implementation and strict quality assurance, have the potential to allay consumer fears to a significant degree. Once such policies are developed, though, the public must be made more aware of their existence. Currently, only 14 percent of online health seekers “always” read sites’ privacy and ethics statements; 21 percent read them “often”; 36 percent read them “sometimes”; and fully 29 percent “rarely” or “never” review the policies at all.

IX. WHO IS MINDING THE STORE? WHO SHOULD?

Despite the firmly held convictions of the majority of American Internet users about the importance of privacy, there is a paradoxical lack of understanding as to whether Internet privacy is protected (if at all), how it should be regulated (if at all), and who should be responsible for any oversight.

When asked if there are current state or federal laws that protect the privacy and confidentiality of personal medical information on the Internet, 70 percent of all online users responded that they did not know. Six percent responded affirmatively and 24 percent responded negatively.

Figure 13: “Who do you think should be responsible for regulating health sites and the way they use information obtained from visitors?”

ALL ONLINE USERS	
Government	35%
Industry associations	20%
Other	6%
Web sites should not be regulated	8%
Don't know	30%

When asked which types of sites are *currently* most trusted to keep personal health information private and secure, online health users cited institutes (such as the NIH or CDC) and medical associations (such as the AMA) highest, and Web portals and online drugstores lowest. Most significant about this finding is that not one single type of site was trusted by a majority of respondents.

Figure 14: Health seekers indicating a moderate or high level of trust that these sites would keep personal information private.

ONLINE HEALTH SEEKERS	
Institutes (NIH, etc.)	44%
Medical associations (AMA, etc.)	42%
Hospitals (Mayo Clinic, etc.)	41%
Disease-specific sites	32%
Medical-focused sites	32%
Not-for-profit groups	30%
Patient-run sites	24%
Health sections of major media sites (CNN, etc.)	20%
Online communities (iVillage, etc.)	14%
Pharmaceutical companies or product sites	14%
Portals (Yahoo!, etc.)	14%
Online drugstores	12%

Conclusion

As is true with many studies of technologic change, especially those fraught with significant personal implications for the average citizen, this survey perhaps raises more questions than it answers. Indeed, that was its intent. Nonetheless, certain findings of *Ethics Survey of Consumer Attitudes About Health Web Sites* are definitive and incontrovertible:

- The American Internet user is confused and concerned about online health privacy in equal measure.
- Safeguards for the privacy Americans expect (and indeed treasure) must be developed, but they first must be proposed and discussed in forums that include all stakeholders in the new Internet healthcare arena.
- Any steps taken in this new medium must be as innovative as the medium itself.

For pharmaceutical companies, insurance companies, HMOs, pure-play online ventures, provider networks, and others, this innovation must spring from listening intently and continuously to the desires and concerns of consumers. The online medium gives every company the ability to hear the voices of individual consumers and react to them on a one-to-one level, in near-real time. To educate and assuage in the realm of privacy, the following suggestions represent a jumping-off point for all e-health players:

- Display your privacy policy prominently and in clear language. Market it, educate your consumers about it, and most important, follow it.
- If your company falls into one of the less-trusted categories, make it your long-term goal to redefine consumer perceptions of your brand through the Internet, where that feat has already been proven possible. To begin, consider forming a relationship with a better-trusted partner, such as a network of doctors.
- Become a vocal proponent of privacy protection and education by proudly sponsoring elements of the privacy debate that emanate far beyond the niche of your traditional business. Face this issue head-on rather than dancing around it, and let consumers know that you are doing so.
- Succeed professionally by behaving ethically. In the increasingly consumer-facing realm of online healthcare, responsible, consumer-friendly information handling will mark the long-term winners.