

# Health Care Consumers' Preferences Around Health Information Exchange

Rina V. Dhopeswarkar, MPH<sup>1</sup>

Lisa M. Kern, MD, MPH<sup>2,3</sup>

Heather C. O'Donnell, MD, MS<sup>4</sup>

Alison M. Edwards, MStat<sup>2</sup>

Rainu Kaushal, MD, MPH<sup>1-3,5</sup>

<sup>1</sup>Department of Pediatrics, Weill Cornell Medical College, New York, New York

<sup>2</sup>Department of Public Health, Weill Cornell Medical College, New York, New York

<sup>3</sup>Department of Medicine, Weill Cornell Medical College, New York, New York

<sup>4</sup>Department of Pediatrics, Albert Einstein College of Medicine/Children's Hospital at Montefiore, Bronx, New York

<sup>5</sup>New York Presbyterian Hospital, New York, New York



MORE ONLINE  
www.annfamned.org

Conflicts of interest: authors report none.

## CORRESPONDING AUTHOR

Rina V. Dhopeswarkar, MPH  
Division of Quality and Medical Informatics  
Weill Cornell Medical College  
402 E 67th St, Ste 301  
New York, NY 10065  
rdhopes@gmail.com

## ABSTRACT

**PURPOSE** Consumer buy-in is important for the success of widespread federal initiatives to promote the use of health information exchange (HIE). Little is known, however, of consumers' preferences around the storing and sharing of electronic health information. We conducted a study to better understand consumer preferences regarding the privacy and security of HIE.

**METHODS** In 2008 we conducted a cross-sectional, random digit dial telephone survey of residents in the Hudson Valley of New York State, a state where patients must affirmatively consent to having their data accessed through HIE.

**RESULTS** There was an 85% response rate (N = 170) for the survey. Most consumers would prefer that permission be obtained before various parties, including their clinician, could view their health information through HIE. Most consumers wanted any method of sharing their health information to have safeguards in place to protect against unauthorized viewing (86%). They also wanted to be able to see who has viewed their information (86%), to stop electronic storage of their data (84%), to stop all viewing (83%), and to select which parts of their health information are shared (78%). Among the approximately one-third (n = 54) of consumers who were uncomfortable with automatic inclusion of their health information in an electronic database for HIE, 78% wished to approve all information explicitly, and most preferred restricting information by clinician (83%), visit (81%), or information type (88%).

**CONCLUSION** Consumers in a state with an opt-in consent policy are interested in having greater control over the privacy and security of their electronic health information. These preferences should be considered when developing and implementing systems, standards and policies.

*Ann Fam Med* 2012;10:428-434. doi:10.1370/afm.1396.

## INTRODUCTION

Health information exchange (HIE), the exchange of electronic health information across health care clinicians and organizations, has the potential to improve health care quality delivered by the US health care system.<sup>1</sup> The federal government has undertaken an approximately \$30 billion initiative to promote the adoption and meaningful use of electronic health records (EHRs) capable of HIE.<sup>2,3</sup> For HIE to be effective, physicians must use a HIE to look up their patients. Because many states require consent before any personal health information can be disclosed or electronically accessed,<sup>4,5</sup> it is equally important that patients are comfortable with an HIE. Studies have shown that although American consumers are supportive of HIE and believe it has the potential to improve health care delivery, they have concerns regarding the privacy and security of their health data.<sup>6-8</sup> Little is known, however, about what features, safeguards, and policies would help consumers to feel more comfortable with the privacy and security of their electronic health information.

To be able to describe consumer's detailed preferences for the privacy and security of their health information, we conducted a survey of con-

sumers' attitudes toward the use of EHRs and HIE in a community that is a national leader in EHR adoption and HIE initiatives<sup>9,10</sup> and has high levels of consumer support of HIE.<sup>11</sup>

## METHODS

### Study Design and Population

We conducted a cross-sectional survey of consumers' opinions on EHRs and HIE among 170 health care consumers in the Hudson Valley region of New York State, a state where patients must consent to having their data accessed through HIE.<sup>12</sup> Eligible participants included English-speaking residents of the 8 counties immediately north of Manhattan. This study was approved by the Institutional Review Board of Weill Cornell Medical College.

### Data Collection

Details of the sampling methods have been described previously.<sup>11</sup> A random digit dial telephone survey restricted to landline numbers was administered by the Cornell Survey Research Institute in January-April 2008. The target sample size was 150 based on power calculations regarding the expected precision of the rate of support for HIE (71.5% ± 7.25%). Respondents provided verbal consent and received \$10 for completing the survey.

### Questionnaire

The structured questionnaire was developed with input from a team with expertise in medical informatics, health services research, and consumer advocacy.<sup>11</sup> Questions assessing consumer's attitudes were modeled after existing national consumer surveys on HIE.<sup>13-16</sup> The questionnaire was pilot tested among 25 ambulatory patients in the outpatient clinics of the Cornell Internal Medicine Associates.<sup>11</sup> The full questionnaire consisted of 42 questions<sup>11</sup> that assessed respondents' demographic characteristics, self-reported health, use of health care services, use of the Internet, and perceptions and opinions regarding the use of EHRs and HIE, including privacy and security preferences for HIE, as well as perceptions and experiences of accessing personal health information online. A subset of 13 questions from the full 42-question survey was analyzed for this study.

In our survey questionnaire (Supplemental Appendix, available at <http://annfam.org/content/10/5/428/suppl/DC1>), an EHR was described as a record that can be created, stored, and viewed on a computer and that contains a patient's medical information, including notes from health care visits, laboratory and radiology tests, prescribed medications, health insurance, and information to allow for correct patient

identification. HIE was described to respondents as having one's EHR (or information that would be contained in an EHR) shared and viewed electronically by different clinicians involved in their care. We described 3 potential HIE architecture models and asked respondents whether they were comfortable with each (yes/no). The options described were as follows: (1) health information stored on a small card that could be carried by patients to medical visits and read by clinicians using special machines; (2) health information kept at the different locations where the patient was seen that could be sent individually over a secure connection directly from one doctor to another; and (3) health information kept electronically in one central database that the patients' clinicians could access to read and add to using a password-protected, secure connection. To assess preferences about the storage of health information for the purpose of HIE, respondents were asked whether they would want all their health information to be stored automatically in a password-protected, secure central repository that their clinician could access, similar to option 3 above. Respondents who indicated that they would not want automatic storage of their information in this manner were asked follow-up questions about the types of restrictions they would want to regulate what information gets included in the database.

Because the central HIE database model would theoretically pose the greatest privacy and security risk to their electronic health information, patients were asked to consider this model when answering the following questions. Respondents were asked which of the following parties they would trust the most to regulate the database and keep it secure: health plan, office practices or doctors' organizations, hospitals, government, or other. Respondents were also asked whether they would want various parties to view their information in the database and whether their permission would be required for viewing. Respondents were then asked how long a doctor should have access to their health information once permission was granted (forever, until permission is taken away, for 1 year, or for 1 week after my visit).

Respondents were asked to rate the importance of the following protections: "safeguards against unauthorized viewing of my medical record," "the ability to see who has viewed my electronic medical record," "the ability to choose which parts of my medical record would be shared electronically," "the ability to stop my information from being stored electronically," and "the ability to stop all viewing of my electronic information."

### Statistical Analysis

Univariate statistics were used to describe the distribution of respondent's demographic characteristics and

their preferences for the storage, sharing, and safeguarding of their medical information. During analyses, we dichotomized question responses that assessed importance of various safeguards of HIE into "essential or important" and "somewhat or not important." We explored bivariate associations between respondent characteristics and willingness to have data automatically stored in a central repository using Fischer's exact test. Variables significantly associated with the outcome were selected for inclusion in the multivariable logistic regression model. We used backward stepwise elimination to determine the final model. Data analysis was performed using SAS statistical software (SAS 9.3, SAS Institute).

## RESULTS

### Study Population

Of the 199 people reached by telephone, 170 (85%) completed the survey.<sup>11</sup> Age within this group varied, with 36% of respondents reporting they were aged between 25 and 44 years, and 40% were aged between 45 to 64 years. Most respondents were white (81%) and had at least 2 years of education beyond high school (82%). One-third had an annual household income of \$100,000 or higher, and 82% had Internet access at either their home or work (Table 1). As reported in a previous study that examined a separate topic from the same survey, the demographic characteristics of our study sample are fairly similar to the entire Hudson Valley population, as reported through 2009 census data, in terms of race, age and income.<sup>11,17</sup>

### Preferences for Storing and Sharing Health Information

Respondents were generally comfortable with the 3 HIE architecture models described (Table 2). Most were comfortable with storage of health information on an editable, readable portable device (83%) and at different locations with data shared over a secure Internet connection (79%). Fewer were comfortable with storage of information on a single, central database that can be accessed over a secure password-protected connection (68%) when compared with a portable device (68% vs 83%,  $P = .02$ ) and when compared with different locations (68% vs 79%,  $P = .003$ ).

### Preferences for Including Health Information in an HIE

Two-thirds of consumers ( $n = 111$ ) indicated that they were comfortable with automatic storage of their health information in a central database so that it may be accessed by clinicians through an HIE (Table 2). Among the one-third of respondents who would not

want automatic storage of their information, most wanted to restrict the storage of their information by visit type, information type, and by clinician (Table 2). Results of multivariable logistic regression showed that male respondents (odds ratio [OR] = 2.2; 95% confidence interval [CI], 1.1-4.6) and those who believed that a secure Internet connection is secure (OR = 3.0; 95% CI, 1.3-6.9) were more likely to be willing to have their health information stored automatically in a central database.

### Entity Responsible for Health Information Storage, Maintenance, and Security

About one-half of the respondents (51%) said they would trust their physicians' practice or organization to regulate the privacy and security of a database that contains their health information (Table 2). Far fewer indicated that they would trust their health plan, hospitals, or the government. Among those who answered

**Table 1. Demographic Characteristics of Sample Population (N = 170)**

Characteristic	All Respondents No. (%) <sup>a</sup>
Sex, female	91 (54)
Race <sup>b</sup>	
White	138 (81)
Black	13 (8)
Other	9 (5)
Missing or refused	10 (6)
Age, y	
18-24	10 (6)
25-44	60 (36)
45-64	67 (40)
65 or older	32 (19)
Annual household income <sup>b</sup>	
<\$30,000	28 (17)
\$30,000 to \$60,000	36 (21)
\$61,000 to \$80,000	25 (15)
\$81,000 to \$100,00	15 (9)
>\$100,000	54 (32)
Missing or refused	12 (7)
Education level <sup>b</sup>	
≤8 <sup>th</sup> grade	1 (1)
Some high school, did not graduate	3 (2)
High school graduate or GED	25 (15)
Some college or 2-year degree	54 (32)
≥4-year college graduate	84 (50)
Missing or refused	3 (2)
Internet access available at work or home	139 (82)

GED = General equivalency diploma.

<sup>a</sup> Percentages may not sum to 100% because of rounding; and numbers may not sum to 170 because of missing responses.

<sup>b</sup> Missing responses indicated.

**Table 2. Consumers' Preferences for Storing and Sharing Health Information**

Preference	No. (%) <sup>a</sup>
Methods for storing and sharing health information with which respondents were comfortable <sup>b</sup>	
On an editable and readable portable device (n = 169)	140 (83)
At different locations and shared over a secure connection (n = 165)	131 (79)
On a single, central database and shared over a secure connection with the use of a password (n = 162)	110 (68)
Interest in automatic storage of medical information in a database (n = 165) <sup>c</sup>	
Yes	111 (67)
No	54 (33)
If not interested in automatic storage, preferences for restricting electronic storage of health information in a database (n = 54) <sup>b,c</sup>	
Determine which clinicians send information that will be included	45 (83)
Determine what types of medical information are included (test results, medication information, etc)	49 (91)
Determine which health care visits will be included (outpatient visit, emergency department visit, hospital stays, etc)	46 (85)
Approve every piece of information	42 (78)
Parties most trusted to regulate the privacy and security of the database (n = 152) <sup>c</sup>	
Office practice or physicians organization	76 (50)
Other	31 (18)
Health plan	24 (16)
Hospitals	11 (7)
Government	10 (7)
Length of time physician should be able to access health information through HIE after permission has been given by the patient (n = 167) <sup>c</sup> :	
One week after patient's visit with physician	39 (23)
One year after permission is given	27 (16)
Continuous access until permission is taken away	94 (56)
Indefinite access	7 (4)
Parties that should be able to view health information in the case of a medical emergency when permission cannot be obtained (n = 168) <sup>b,c</sup>	
Designated family member or friends	156 (93)
Primary care doctor	158 (93)
Other doctors or clinicians (in emergency department or hospital, etc)	138 (82)
No one should access my health information without my permission even in a medical emergency	21 (13)

<sup>a</sup> Percentages may not sum to 100 because of rounding and numbers may not sum to 170 because of missing responses. Actual denominators indicated in parentheses after row entries.

<sup>b</sup> Respondents were asked to select all options that applied.

<sup>c</sup> Respondents were asked to consider a system where their medical information from different health care visits and clinicians is stored on a central electronic database that their doctors can access (health information exchange, HIE) with their permission.

"other," a few respondents (10%) indicated that they would not trust anyone other than themselves.

### Protections Against Unauthorized Viewing of Health Information

More than three-quarters of all respondents considered every safeguard feature around HIE either essential or important (Figure 1). Many of these safeguards related to preventing unauthorized viewing and sharing of their health information. When asked whom they would allow to view their health information through

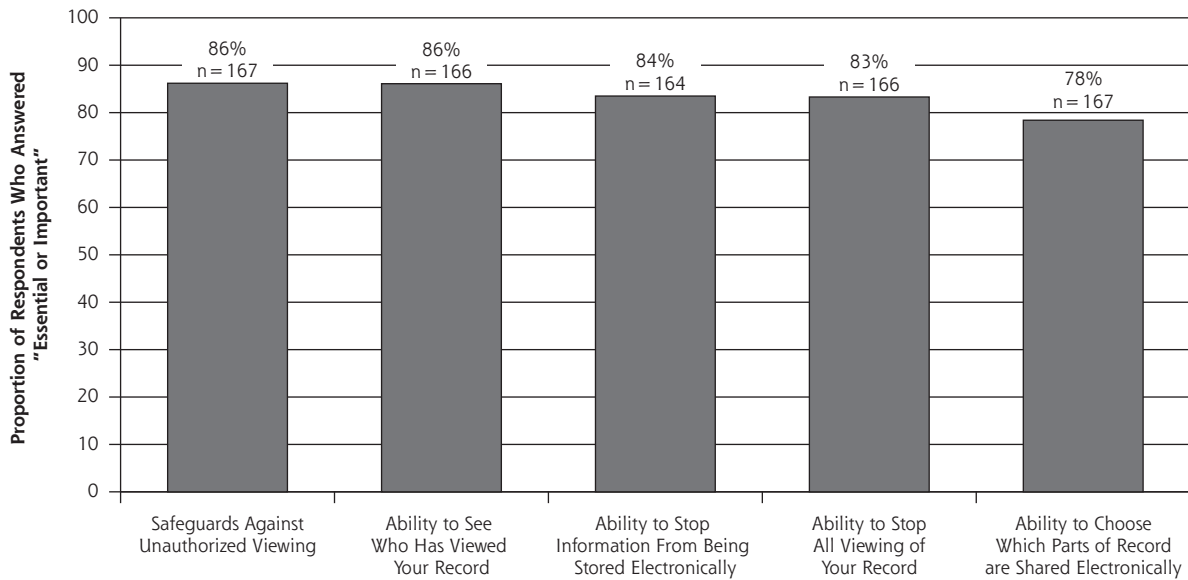
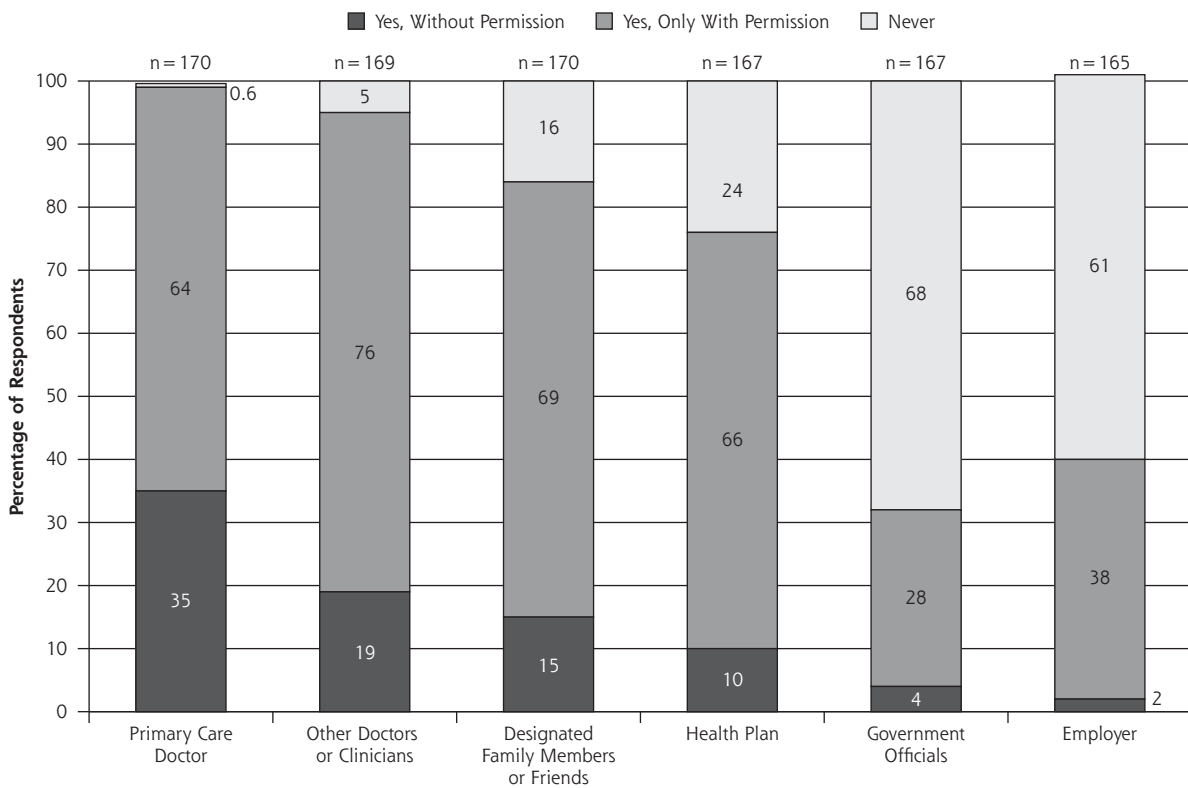
HIE and whether their permission should be required for viewing by that party, consumers were more likely than not to indicate that their permission would be required (Figure 2). Respondents were most comfortable with having their primary care doctor view their health information without their permission (35%) and least comfortable with government officials (4%) and employers (2%). When asked about the length of time their doctor should be able to access their health information through HIE once that doctor has been given permission to view it (Table 2), more than one-half of respondents said that they would want their doctor to have continuous access until they revoke permission. Less than one-quarter would want their doctor to have access for 1 week after their visit with them, or for 1 year after permission was given. Less than 5% of consumers would want their doctor to have indefinite access. In the case of a medical emergency for which their permission could not be obtained, most respondents would allow their primary care doctor (93%), their designated family members or friends (93%), and other doctors or clinicians who care for them (82%) to view their health information (Table 2).

### DISCUSSION

We found that more than two-thirds of people surveyed in this community were supportive of HIE and willing to have their health information automatically stored in an HIE. Men and those who felt secure using a secure Internet connection were more likely to be supportive of automatic inclusion of their health information. One-third of respondents

were not willing to have their data stored automatically and expressed a preference for a high degree of control over their data, including control over the type of information stored. Most respondents wanted safeguards against unauthorized viewing of their information. We also found that most respondents indicated comfort with all 3 described HIE architecture models (portable device, data residing in multiple locations, and a centralized database).

Given the highly sensitive nature of health information and the consequences that can occur in the event

**Figure 1. Privacy: features consumers want for safeguarding their medical information.****Figure 2. Consumers' preferences regarding permission to view electronic health information.**

Note: Top numbers represent the total number of respondents replying to each question.

of its disclosure,<sup>18</sup> it is not surprising that consumers in this study expressed strong concerns regarding the unauthorized viewing of their electronic health infor-

mation. Consent policies that would allow consumers to control what, by whom, and for how long their health information could be accessed may allay these

concerns. New York State, in which this study took place, has an opt-in approach to consent.<sup>12</sup> That is, patients must actively provide informed consent for clinicians to access to their HIE data.<sup>4</sup> Some health information organizations across the nation have adopted opt-out patient consent models, in which patients are included in an HIE unless they specifically request otherwise. The views of those patients are not clear, and future studies should seek to understand them better. Our findings, including having one-third of respondents preferring a high degree of control over data, are consistent with this state's opt-in approach.

Implementing appropriate consent policies and technical guidelines regarding use of EHRs and an HIE could potentially improve the security of patients' health information compared with traditional paper records.<sup>19</sup> There are state and federal organizations engaged in identifying technical standards and consistent privacy policies to facilitate and protect HIE, such as the Standards and Interoperability Framework committee.<sup>20</sup> Ensuring that HIE standards and policies incorporate consumer preferences, and expanding the scope of consumer engagement and education campaigns around an HIE will be key in gaining the public's trust.

Our findings suggest that consumers support any of 3 HIE architectural models. Although centralized database systems may be the most user-friendly,<sup>21</sup> they were slightly less popular among consumers than storage on a portable device or at different locations, perhaps because centralized databases were believed to have the highest likelihood of security breaches.<sup>22</sup> The portable device model has not been widely implemented in the United States,<sup>21</sup> although a portable electronic health card was pilot tested in Germany but stalled when providers were unwilling to buy the necessary equipment to read the cards.<sup>23,24</sup> Similar obstacles might prevent such a model from being implemented in the United States despite our study showing consumers' interest in it. Most respondents were comfortable with storage of health information at the site where care was received with transmission over a secure connection. This finding is an encouraging, as this model is similar to the architecture model of the Direct Project, an HIE service being developed by the federal government that involves sending encrypted health information directly to known, authenticated recipients over the Internet.<sup>25</sup> Those consumers who were not willing to have all of their data automatically stored in a central repository expressed a willingness to have some specific types of data shared. This finding may have undesirable implications for the utility of HIE, because if many consumers request many different restrictions, then the HIE is less complete, less useful, and possibly harmful (if the missing data are

clinically important). Willingness to have data automatically stored was associated with being male and believing a the Internet connection is secure. These results are surprising because in previous studies sex has not been significantly associated with support of physician or personal use of HIE.<sup>11,26</sup>

Most consumers indicated that they would want their doctors to have access to their health information in an emergency, even if they cannot give permission. In New York, this preference is addressed by "break the glass" provisions that allow for health information to be accessed by a clinician who is treating a patient during an emergency.<sup>12</sup> High levels of support of HIE use by physicians during emergencies may be related to advertising campaigns launched across the country to educate consumers about the importance and utility of an HIE during emergencies.<sup>27</sup> Consumers expressed greatest trust in their own doctor's practice to regulate the privacy and security of their electronic health information. In New York, a statewide collaboration process resulted in a white paper with recommendations for standard policies around HIE privacy and security.<sup>12</sup> According to these recommendations, establishment and enforcement of these policies are the responsibility of health information organizations as opposed to individual physicians or practices.<sup>12</sup> Health information organizations across the country are also taking on responsibilities of governing the privacy and security of data within an HIE.<sup>4</sup> Because our survey did not explicitly ask respondents about health information organizations, future studies should explore further consumers' trust in these organizations.

### Study Limitations

Our survey was conducted in a fairly homogenous community, with a population that may not be generalizable to all health care consumers. Given the current federal initiatives to promote health information technology, however, more communities will likely be adopting EHRs and engaging in an HIE, and they may benefit from these findings. Second, although random digit dialing was used to minimize selection bias, unlisted or cellular telephone numbers were not included in our sample. Additionally, although our response rate was high, we were unable to collect any information on nonrespondents, limiting our ability to comment on the extent of any response bias. Third, our survey was conducted before the release of New York Health Information Security and Privacy Collaboration's recommended standard privacy and security policies.<sup>12</sup> Finally, our survey described an EHR as including both patient identifiers and medical information, because the patient identifiers are often required for patient matching. This description could have con-

tributed to respondents' concerns around security of an HIE and may or may not have introduced bias. Future studies could determine whether alternate wording would elicit similar or different responses.

Consumer buy-in is necessary for the success of national HIE initiatives. Our study, among the first to examine the privacy and security-related preferences of consumers in a community where HIE is underway, found that consumers desire greater control over their electronic health information. To address consumers' concerns about the exchange of their health information, their preferences should be incorporated into future iterations of HIE standards and consent policies.

To read or post commentaries in response to this article, see it online at <http://www.annfamned.org/content/10/5/428>.

**Key words:** electronic health records; health information exchange; consumer preference

Submitted June 12, 2011; submitted, revised January 6, 2012; accepted January 13, 2012.

**Funding support:** This work was funded by the Taconic Independent Practice Association.

**Previous presentation:** This work was previously presented as a poster at the American Medical Informatics Association Annual Symposium, November 14-18, 2009, San Francisco, California.

## References

- Institute of Medicine. *Crossing the Quality Chasm: A New Health System for the 21st Century*. Washington, DC: National Academy Press; 2001.
- United States House of Representatives & Senate. *The American Recovery and Reinvestment Act of 2009 (ARRA)*. Washington, CD: U.S. Government Printing Office; 2009.
- Steinbrook R. Health care and the American Recovery and Reinvestment Act. *N Engl J Med*. 2009;360(11):1057-1060.
- Goldstein MM, Rein AL. *Consumer Consent Options for Electronic Health Information Exchange: Policy Considerations and Analysis* [White paper]. Washington, DC: Office of the National Coordinator for Health Information Technology; 2010 March 23.
- Tripathi M, Delano D, Lund B, Rudolph L. Engaging patients for health information exchange. *Health Aff (Millwood)*. 2009;28(2):435-443.
- Markle Foundation. *Attitudes of Americans Regarding Personal Health Records and Nationwide Electronic Health Information Exchange*. Markle Foundation; 2005.
- Wen K-Y, Kreps G, Zhu F, Miller S. Consumers' perceptions about and use of the internet for personal health records and health information exchange: analysis of the 2007 Health Information National Trends Survey. *J Med Internet Res*. 2010;12(4):e73.
- Simon SR, Evans JS, Benjamin A, Delano D, Bates DW. Patients' attitudes toward electronic health information exchange: qualitative study. *J Med Internet Res*. 2009;11(3):e30.
- Taconic Independent Practice Association (IPA). Website. <http://www.taconicipa.com/>. Accessed Jun 9, 2011
- Taconic Health Information Network and Community Website. <http://www.thincrhio.org/main-page.html>. Accessed Jun 9, 2011
- O'Donnell H, Patel V, Kern LM, et al. Healthcare consumers' attitudes towards physician and personal use of health information exchange. *J Gen Intern Med*. 2011;26(9):1019-1026.
- New York eHealth Collaborative, New York State Department of Health. *Recommendations for Standardized Consumer Consent Policies and Procedures for RHIOs in New York to Advance Interoperable Health Information Exchange to Improve Care*. 2008. [http://nyhealth.org/images/files/File\\_Repository16/pdf/Consent\\_White\\_Paper\\_20081125.pdf](http://nyhealth.org/images/files/File_Repository16/pdf/Consent_White_Paper_20081125.pdf).
- Attitudes of Americans Regarding Personal Health Records and Nationwide Electronic Health Information Exchange. 2005. [http://www.markle.org/sites/default/files/research\\_release\\_101105.pdf](http://www.markle.org/sites/default/files/research_release_101105.pdf). Accessed Jan 27, 2010.
- CAHPS Clinician & Group Survey Adult Primary Care Questionnaire. <http://www.cahps.ahrq.gov/default.asp>. Accessed Jan 27, 2010.
- Ware JE Jr, Kosinski M, Keller SD. A 12-Item Short-Form Health Survey: construction of scales and preliminary tests of reliability and validity. *Med Care*. 1996;34(3):220-233.
- The South Dakota Electronic Health Record Assessment Survey: Health Care Consumer. 2008. <http://www.ehealth.dsu.edu/Resources.aspx>. Accessed Oct 15, 2007
- State and County QuickFacts. Data derived from Population Estimates, Census of Population and Housing, Small Area Income and Poverty Estimates, State and County Housing Unit Estimates, County Business Patterns, Nonemployer Statistics, Economic Census, Survey of Business Owners, Building Permits, Consolidated Federal Funds Report. <http://quickfacts.census.gov>. Accessed Oct 4, 2011
- Gostin L. Health care information and the protection of personal privacy: ethical and legal considerations. *Ann Intern Med*. 1997;127(8 Pt 2):683-690.
- Barrows RC Jr, Clayton PD. Privacy, confidentiality, and electronic medical records. *J Am Med Inform Assoc*. 1996;3(2):139-148.
- Standards & Interoperability (S&I) Framework's Wiki. Tangient, 2011. <http://wiki.siframework.org/>. Accessed Oct 7, 2011.
- Wilcox A, Kuperman G, Dorr DA, et al. Architectural strategies and issues with health information exchange. *AMIA Annu Symp Proc*. 2006:814-818.
- Written statement of Richard Gibson. In: *Hearing on Standards for Health IT: Meaningful Use and Beyond*. Washington, DC: Subcommittee on Technology and Innovation, Committee on Science and Technology; 2010.
- Hoerbst A, Kohl CD, Knaup P, Ammenwerth E. Attitudes and behaviors related to the introduction of electronic health records among Austrian and German citizens. *Int J Med Inform*. 2010;79(2):81-89.
- Germany's electronic health card stalls. *EHealthInsider*. apr 17, 2009. <http://www.ehi.co.uk/news/primary-care/4757>.
- The Direct Project Overview. 2010. <http://wiki.directproject.org/file/view/DirectProjectOverview.pdf>. Accessed Mar 24, 2011.
- Patel VN, Abramson E, Edwards AM, Cheung MA, Dhopeswarkar RV, Kaushal R. Consumer attitudes toward personal health records in a beacon community. *Am J Manag Care*. 2011;17(4):e104-e120.
- Information Stat Campaign. [Website]. <http://www.informationstat.com/main.html>. Accessed Oct 4, 2011