Findings from 2017 on Consumer Health Informatics and Education: Health Data Access and Sharing

Pascal Staccini, Annie Y.S. Lau

Findings from 2017 on Consumer Health Informatics and Education: Health Data Access and Sharing

Pascal Staccini[1], Annie Y. S. Lau[2], Section Editors for the IMIA Yearbook Section on Consumer Health Informatics and Education

[1] INSERM UMR 912 SESSTIM, IRIS Dept, UFR Médecine, Université Nice-Sophia Antipolis, France

[2] Centre for Health Informatics, Australian Institute of Health Innovation, Macquarie University, Australia

Summary

Objective: To summarize the state of the art during the year 2017 in consumer health informatics and education, with a special emphasis on sharing health data and accessing personal health information (PHI) from patients' and consumers' perspective.

Methods: We conducted a systematic search of articles published in PubMed using a predefined set of queries which identified 228 potential articles for review. The section editors then screened these articles according to topic relevance and selected 15 candidate best papers for full review and scoring by a panel of international experts. Based on the scores and the reviews, four papers received the highest score and were selected in a consensus meeting as the best papers on health data access and sharing from consumers' and patients' perspective.

Results: These four papers were categorised into the following topics: 1) data sharing for research and governance in privacy protection; 2) use of personal health information and individual privacy concerns; and 3) consumers' views and demographic characteristics regarding health data sharing and the use of digital health portals. Overall, it was surprising to see only a small number of papers reporting original research in this area.

Conclusions: Patients understand the need for sharing information to facilitate best care and to enrich biomedical knowledge. When confronted with the reality of accessing information systems for their own information, patients are concerned about usability as well as privacy. Overall, there is a need for more emphasis on: 1) considering privacy as a feature defined by design; 2) using specific consent approaches and data sharing mechanisms for recruiting clinical trial participants; 3) taking into account socio-demographic characteristics when promoting consumer access to personal health information; and 4) defining indicators of high-quality care to incorporate healthcare professionals' level of caution when accessing patients' medical information and fostering patient trust in data exchange. Ultimately, privacy mechanisms should be part of the design process and not only be implemented when security has been breached and violated.

Keywords

Consumer health informatics; health data sharing; personal health information; privacy by design; online access to health records

Yearb Med Inform 2018:163-9
http://dx.doi.org/10.1055/s-0038-1641218

1 Introduction

For this 27th edition of the Yearbook of the International Medical Informatics Association (IMIA), the topic of "Between access and privacy: Challenges in sharing health data" is timely, especially when it comes to sharing and accessing personal health data from consumers' and patients' perspective. In 2015, Deneke et al. [1] had already initiated discussion in this area and concluded that: "preserving patient privacy and confidentiality in all environments is a main issue in the context of social-media usage in healthcare and research, as well as providing means for patients or Internet users to express concerns on data usage". However, it took the major Cambridge Analytica/Facebook scandal, three years later, to remind us of the scale and significance of how our personal data can be violated in order to manipulate our views when data security and privacy concerns are left unchecked. As Landau writes [2]: "… the failure to protect users' privacy, the failure to protect voters, and the failure to uncover the actions and violations of laws … may well have affected the Brexit referendum and the U.S. presidential election." When it comes to our health data, are we doing enough to protect our privacy? How can we uphold these privacy principles without obstructing the goodwill in using innovation to facilitate data sharing and access that is essential for optimal healthcare?

Sharing health data is now essential in many international research collaborations and large-scale analytics projects, such as genetics, cancer or other chronic disease registries, substance abuse, public health surveillance, epidemiology, disease tracking, and routine patient care in the emergency department. On May 25th 2018, the General Data Protection Regulation (GDPR), Europe's new framework for data protection laws, has introduced three definitions that pertain to health data[1]. These definitions lay the foundations to guide the process of sharing health data, and include:

- *Data concerning health* defined by the GDPR as "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status."
- *Genetic data* defined as "personal data relating to inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question."

[1] https://gdpr-info.eu

- *Biometric data* defined as "personal data resulting from specific technical processes relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data."

Besides the importance of data sharing in scientific research, data exchange is often essential to achieve optimal healthcare. Patient care should benefit when personal health data can easily, and securely, move from one healthcare provider to another. However, data security concerns are often the reason why healthcare providers are hesitant to share data. Although new regulations allow for information to be exchanged in certain circumstances, including patients being able to access their own medical data (such as via patient portals), whether these portals are designed with 'privacy', how clinicians react to such data access by patients, and consumers' considerations need to be addressed in order to facilitate meaningful use and access.

Focusing on patient's perceptions and expectations, we have reviewed current literature related to two patients-centric topics: providing and sharing data for research, and accessing personal health information in clinical care. The aim was to highlight papers published in 2017 and select the best papers representative of this topic.

2 Methodology

We used PubMed to conduct our review. Following the methodology from previous years, we used the following queries to capture relevant papers in health data access and sharing from consumers' and patients' perspectives. The search strategy is detailed below:

Query 1. ((2017[DP] NOT pubstatusaheadofprint) NOT Bibliography[pt] NOT Comment[pt] NOT Editorial[pt] NOT Letter[pt] NOT News[pt] NOT Case Reports[pt] NOT Published Erratum[pt] NOT Historical Article[pt] NOT Legal Cases[pt] NOT legislation[pt] NOT ("review"[Publication Type] OR "review literature as topic"[MeSH Terms] OR "literature review"[All Fields]))

Query 2. AND ("access"[All Fields] OR "sharing"[All Fields] OR "share"[All Fields] OR "data sharing" [All Fields] OR "data share"[All Fields] OR "open data"[All Fields] OR "information sharing"[All Fields] OR "access to information"[All Fields] OR "health exchange"[All Fields] OR "data access"[All Fields] OR "open access"[All Fields] OR "dissemination"[All Fields] OR "sharing practices" [All Fields] OR "data protection"[All Fields] OR "disclosure"[All Fields] OR "information dissemination"[Mesh] OR "data collection"[Mesh])

Query 3. AND ("patient data"[All Fields] OR "patient generated data"[All Fields] OR "quantified-self"[All Fields] OR "quantified self"[All Fields] OR "consumer health information"[All Fields] OR "patient's medical information"[All Fields] OR "personal data"[All Fields] OR "health data"[All Fields] OR "self-tracking tool"[All Fields] OR "self-experimentation"[All Fields] OR "research dataset"[All Fields] OR "research dataset"[All Fields] OR "electronic health record"[All Fields] OR "electronic medical record"[All Fields] OR "personal health record"[All Fields] "personal health information"[All Fields] OR "personal medical record" [All Fields] OR "health record"[All Fields] OR "medical record"[All Fields] OR "medical data"[All Fields] OR "clinical data"[All Fields] OR "patient portal"[All Fields] OR "EHR"[All Fields] OR "PHR"[All Fields] OR "electronic patient record"[All Fields] OR "EPR"[All Fields] OR "PHI"[All Fields] OR "electronic health"[All Fields] OR "patient record"[All Fields])

Query 4. AND ("privacy"[All Fields] OR "protection"[All Fields] OR "informed consent"[All Fields] OR "private" [All Fields] OR "privacy"[Mesh])

Query 5. AND ("social media"[All Fields] OR "facebook"[All Fields] OR "twitter"[All Fields] OR "youtube"[All Fields] OR "social network site"[All Fields] OR "social web"[All Fields] OR "online social network"[All Fields] OR "social environment"[All Fields] OR "social process"[All Fields] OR "social competition"[All Fields] OR "social norm"[All Fields] OR "social feedback"[All Fields] OR "social influence"[All Fields] OR "social comparison"[All Fields] OR "social network"[All Fields] OR "discussion group"[All Fields] OR "support group"[All Fields] OR "social support"[All Fields] OR "community network"[All Fields] OR "online community"[All Fields])

Table 1 outlines results from different combinations of the five query components. It must be noted that the combination of all five query components returns only five articles, resulting in only one article relevant to our topic [3]. Although the fifth query component was specifically related to "social media", we decided to eliminate it in our final research strategy in order to return more articles. This means that the final query was the combination of the first four query components, which returned 228 articles.

Table 1 Results of the various combinations of search query components (Pubmed retrieval).

Query					Number of retrieved articles
1	2	3	4	5	
X					995,656 articles
X	X				112,041 articles
X	X	X			3621 articles
X	X	X	X		228 articles
X	X	X	X	X	5 articles

Abstracts of these 228 articles were screened and assessed according to: 1) the level of relevance regarding the 2018 yearbook topic "Between Access and Privacy: Challenges in Sharing Health Data"; 2) the nature of the problem addressed, such as legal aspects and requirements, methods and tools, and healthcare topic, 3) the level of evidence if appropriate, and 4) the level of innovation in the approach presented. After screening, 15 papers were selected and presented for review and scoring by a panel of external international experts. The four papers that received the highest score, and were agreed upon in a consensus meeting, were selected to be the best papers representative of health data access and sharing from consumers' and patients' perspective.

Table 2 Best paper selection of articles for the IMIA Yearbook of Medical Informatics 2018 in the section 'Consumer Health Informatics and Education'. The articles are listed in alphabetical order of the first author's surname.

Section
Consumer Health Informatics and Education
▪ Bender JL, Cyr AB, Arbuckle L, Ferris LE. Ethics and Privacy Implications of Using the Internet and Social Media to Recruit Participants for Health Research: A Privacy-by-Design Framework for Online Recruitment. J Med Internet Res 2017 Apr 6;19(4):e104.
▪ Peacock S, Reddy A, Leveille SG, Walker J, Payne TH, Oster NV, Elmore JG. Patient portals and personal health information online: perception, access, and use by US adults. J Am Med Inform Assoc 2017 Apr 1;24(e1):e173-e177.
▪ Sanderson SC, Brothers KB, Mercaldo ND, Clayton EW, Antommaria AHM, Aufox SA, Brilliant MH, Campos D, Carrell DS, Connolly J, Conway P, Fullerton SM, Garrison NA, Horowitz CR, Jarvik GP, Kaufman D, Kitchner TE, Li R, Ludman EJ, McCarty CA, McCormick JB, McManus VD, Myers MF, Scrol A, Williams JL, Shrubsole MJ, Schildcrout JS, Smith ME, Holm IA. Public Attitudes toward Consent and Data Sharing in Biobank Research: A Large Multi-site Experimental Survey in the US. Am J Hum Genet 2017 Mar 2;100(3):414-27.
▪ Walker DM, Johnson T, Ford EW, Huerta TR. Trust Me, I'm a Doctor: Examining Changes in How Privacy Concerns Affect Patient Withholding Behavior. J Med Internet Res 2017 Jan 4;19(1):e2.

3 Results

Despite the fact that "social networks" or "social media" were topics often used in the 228 retrieved papers, many papers were not related to these topics after a close examination. The 15 candidate best papers are grouped according to the following areas: 1) privacy implications and data sharing for research (online recruitment, biobanking, and clinical trials data reuse) [3-5]; 2) privacy concerns and use of personal health information [6-12]; and 3) general considerations regarding portal use and individual characteristics [13-17].

The selected best papers in the first group, "Privacy implications and data sharing in research", are [3] and [5]. There is one best paper [11] in the second group, "Privacy concerns and use of personal health information", and one best paper [17] in the third group, "General considerations regarding portal use and personal characteristics".

4 Conclusions

Regarding the conclusions of these selected papers, it should not be forgotten that privacy as an ethical concept and as a fundamental human right is not static. Privacy concerns and expectations of research participants are likely to evolve in the coming years as the implications of data-intensive health research and the computerization of health data become better understood by stakeholders. Despite new rule frameworks, constraints, and monitored actions applied to personal and massive data owners, privacy breaches cannot be eliminated, and consumers and patients need to become more aware of the necessity for their data to be protected while making use of the benefits of data exchange and sharing.

Patients, consumers, and healthcare professionals need to be educated on good practices of data sharing and access. In particular, there is a need for more emphasis on: 1) considering privacy as a feature defined by design; 2) using specific consent approaches and data sharing mechanisms for recruiting clinical trial participants; 3) taking into account socio-demographic characteristics when promoting consumer access to personal health information; and 4) defining indicators of high-quality care to incorporate healthcare professionals' level of caution when accessing patients' medical information and fostering patient trust in data exchange. Ultimately, privacy mechanisms should be part of the design process and not only be implemented when security has been breached and violated.

References

1. Denecke K, Bamidis P, Bond C, Gabarron E, Househ M, Lau AYS, et al. Ethical Issues of Social Media Usage in Healthcare. Yearb Med Inform 2015;10:137-47.
2. Landau S. What Went Wrong? Facebook and 'Sharing' Data with Cambridge Analytica. March 28, 2018. https://cacm.acm.org/blogs/blog-cacm/226442-what-went-wrong-facebook-and-sharing-data-with-cambridge-analytica/fulltext (last visit: 16.06.2018)
3. Bender JL, Cyr AB, Arbuckle L, Ferris LE. Ethics and Privacy Implications of Using the Internet and Social Media to Recruit Participants for Health Research: A Privacy-by-Design Framework for Online Recruitment. J Med Internet Res 2017 Apr 6;19(4):e104.
4. Ohmann C, Banzi R, Canham S, Battaglia S, Matei M, Ariyo C, et al. Sharing and reuse of individual participant data from clinical trials: principles and recommendations. BMJ Open. 2017 Dec 14;7(12):e018647.
5. Sanderson SC, Brothers KB, Mercaldo ND, Clayton EW, Antommaria AHM, Aufox SA, et al. Public Attitudes toward Consent and Data Sharing in Biobank Research: A Large Multi-site Experimental Survey in the US. Am J Hum Genet 2017 Mar 2;100(3):414-27.
6. Abdelhamid M, Gaia J, Sanders GL. Putting the Focus Back on the Patient: How Privacy Concerns Affect Personal Health Information Sharing Intentions. J Med Internet Res 2017 Sep 13;19(9):e169.
7. Entzeridou E, Markopoulou E, Mollaki V. Public and physician's expectations and ethical concerns about electronic health record: Benefits outweigh risks except for information security. Int J Med Inform 2018 Feb;110:98-107.
8. Kim KK, Sankar P, Wilson MD, Haynes SC. Factors affecting willingness to share electronic health data among California consumers. BMC

Med Ethics 2017 Apr 4;18(1):25.
9. Lee BS, Oster NV, Chen GY, Ding LL, Walker JD, Elmore JG. Ophthalmology patients' interest in online access to clinic notes at three US clinics. Ophthalmic Physiol Opt 2017 Jul;37(4):420-7.
10. Medford-Davis LN, Chang L, Rhodes KV. Health Information Exchange: What do patients want? Health Informatics J 2017 Dec;23(4):268-78.
11. Peacock S, Reddy A, Leveille SG, Walker J, Payne TH, Oster NV, et al. Patient portals and personal health information online: perception, access, and use by US adults. J Am Med Inform Assoc 2017 Apr 1;24(e1):e173-e177.
12. Rau HH, Wu YS, Chu CM, Wang FC, Hsu MH, Chang CW, et al. Importance-Performance Analysis of Personal Health Records in Taiwan: A Web-Based Survey. J Med Internet Res 2017 Apr 27;19(4):e131.
13. Dhir A, Torsheim T, Pallesen S, Andreassen CS. Do Online Privacy Concerns Predict Selfie Behavior among Adolescents, Young Adults and Adults? Front Psychol 2017 May 23;8:815.
14. Garcia D. Leaking privacy and shadow profiles in online social networks. Sci Adv 2017 Aug 4;3(8):e1701172.
15. Sakaguchi-Tang DK, Bosold AL, Choi YK, Turner AM. Patient Portal Use and Experience Among Older Adults: Systematic Review. JMIR Med Inform 2017 Oct 16;5(4):e38.
16. Trachtenbarg DE, Asche C, Ramsahai S, Duling J, Ren J. The benefits, risks and costs of privacy: patient preferences and willingness to pay. Curr Med Res Opin 2017 May;33(5):845-51.
17. Walker DM, Johnson T, Ford EW, Huerta TR. Trust Me, I'm a Doctor: Examining Changes in How Privacy Concerns Affect Patient Withholding Behavior. J Med Internet Res 2017 Jan 4;19(1):e2.

Correspondence to:
Pascal Staccini
Département IRIS
Faculté de Médecine
Université Nice-Sophia Antipolis
28 avenue de Valombrose,
06107 Nice Cedex 2, France
Email: pascal.staccini@unice.fr

Appendix: Content Summaries of Selected Best Papers for the IMIA Yearbook 2018, Section Consumer Health Informatics and Education

Bender JL, Cyr AB, Arbuckle L, Ferris LE

Ethics and Privacy Implications of Using the Internet and Social Media to Recruit Participants for Health Research: A Privacy-by-Design Framework for Online Recruitment

J Med Internet Res 2017 Apr 6;19(4):e104

New Internet alternatives are explored by health researchers to recruit people for research studies. The increasing use of social networking sites offers easier access to many kinds of populations. They are also economical and more flexible than former ways. However, the use of social media as an online research recruitment tool raises unique ethical issues regarding knowledge and consent before enrolment. It may pose threats to the principles of Respect for Persons and Concern for Welfare in regard to privacy and the individual's right to control information about him/herself. There is only one known study that describes the ethical challenges of social networking and online recruitment for HIV research which conclusions consisted of a set of recommended best practices for HIV researchers. This paper describes how to use the Internet and social media to recruit cancer patients and their family caregivers for a focus group study on dietary self-management behaviors, the ethical concerns raised by the institutional Research Ethics Board (REB), and the privacy-enhancing strategies developed to address them. Two REB questions were to be answered: "How will you inform users about the potential for privacy breaches and their implications? How will you protect users from privacy breaches or inadvertently sharing potentially identifying information about themselves?" In order to elaborate the social media recruitment strategy, a Privacy by Design (PbD) framework was used. It was developed by the former Information and Privacy Commissioner of Ontario, Canada, in the late 1990s. PbD is based on the following seven foundational principles: (1) Proactive not Reactive, Preventative not Remedial (PbD seeks to anticipate and prevent privacy-invasive events before they happen. PbD does not wait for privacy risks to materialize nor offer remedies after the fact); (2) Privacy as the Default Setting (PbD seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected. No action is required on the part of individuals to protect their privacy. It is built in the system, by default.); (3) Privacy Embedded into Design (PbD is embedded into the design and architecture of the system. It is not bolted on as an add-on, after the fact. Privacy is integral to the system, without diminishing functionality.); (4) Full Functionality — Positive-Sum, not Zero-Sum (PbD seeks to accommodate all legitimate interests and objectives in a positive-sum, win-win manner, not through a dated, zero-sum approach where unnecessary tradeoffs are made.); (5) End-to-End Security — Full Lifecycle Protection (PbD explains that strong security measures are essential to PbD from start to finish. Embedding PbD into the system prior to the first element of information being collected ensures that all data are securely retained throughout the entire lifecycle of the data involved.); (6) Visibility and Transparency — Keep it Open (PbD seeks to assure all stakeholders that whatever the business practice or technology involved, it is, in fact, operating according to the stated promises and objectives, subject to independent verification.); and (7) Respect for User Privacy — Keep it User Centric (PbD requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options). Applying the principles of Privacy by Design made the authors 1) Inform about privacy risks with privacy notices written in plain language and approved by a plain-language expert using familiar words, not jargon, active voice, and a conversational study to convey information clearly. 2) Protect privacy using privacy-enhanced social media messages and 3) Disabling comment features or moderating comments. The authors provide reflection on the perceived privacy risks associated with their social media recruitment strategy and the appropriateness of the risk mitigation strategies they employed by discussing the following: (1) What are the potential risks and who is at risk? (2) Is cancer considered sensitive personal information? (3) What is the probability of online disclosure of a cancer diagnosis in everyday life? and (4) What are the public's expectations for online privacy and their views about online tracking, profiling, and targeting?

Sanderson SC, Brothers KB, Mercaldo ND, Clayton EW, Antommaria AHM, Aufox SA, Brilliant MH, Campos D, Carrell DS, Connolly J, Conway P, Fullerton SM, Garrison NA, Horowitz CR, Jarvik GP, Kaufman D, Kitchner TE, Li R, Ludman EJ, McCarty CA, McCormick JB, McManus VD, Myers MF, Scrol A, Williams JL, Shrubsole MJ, Schildcrout JS, Smith ME, Holm IA

Public Attitudes toward Consent and Data Sharing in Biobank Research: A Large Multi-site Experimental Survey in the US

Am J Hum Genet 2017 Mar 2;100(3):414-27

Biological samples are an increasingly important tool for research on human diseases and their genetic and physiological causes. To ease the storage of and access to biological samples, many are now stored in biobanks. A major ethical problem for prospective biobanks is how to insure participants are given their consent when it is not known what they are consenting to in terms of future research. Biobank investigators and policy makers need help respectively to govern and revise the regulations on the protection of human research subjects. The authors conducted a large survey of attitudes toward consent and data sharing in biobank research among diverse participants recruited at multiple healthcare systems participating in the Electronic Medical Records and Genomics (eMERGE) Network. Individuals were randomly assigned to one of three hypothetical biobank scenarios. The scenarios were identical except for the details regarding consent type and data sharing approach. In the first scenario, donated samples and data could be used for all kinds of medical research

and data could be shared with approved investigators only ("broad-controlled"). The second and third scenarios contained an alternative consent approach or data sharing policy: in the "tiered-controlled" scenario, the consent process allowed participants to select the types of research for which their samples and data could be used, and in the "broad-open" scenario, data sharing policy allowed de-identified data to be shared through an online database open to the public. A multidisciplinary working group of experts defined three relevant sub-domains to be assessed within the overarching domain of "attitudes towards participating in a biobank:" perceived benefits of participating in the described biobank, concerns about participating in the described biobank, and information needs about the governance of the described biobank (e.g., how decisions are made regarding the use of samples and data). Of 90,000 surveys mailed, 7,672 individuals were ineligible due to invalid address, death, or incapacity, and 681 refused to participate. Of the 82,328 eligible individuals, exactly 13,000 responded (response rate 15.8%). Among responders, 11,712 completed the paper (90.1%) and 1,288 the online (9.1%) survey. Overall, 66% (95% CI: 63%–69%) of participants stated that they would be willing to participate in the biobank described to them. Willingness did not differ between broad and tiered consent models (68% versus 66% respectively, P=0.30). Willingness was slightly higher among participants presented with a controlled rather than an open data sharing model, although the difference was not large in absolute terms (68% versus 65%, respectively, P=0.03). Participant characteristics, independently linked with willingness to participate, before attitudes were entered into the model, were: race (as self-reported by the respondents in the survey), education, religiosity, and trust and privacy concerns. When attitudes toward the biobank were entered into the model, each of the three composite scale variables was independently associated with willingness: participants were more willing to participate if they perceived more benefits, had fewer concerns, and had fewer information needs. In this model, education and religiosity remained associated with willingness, but race, trust, and privacy concerns did not. The results from this study suggest that biobanks using broad consent may not be less successful in recruiting participants than if they use more specific consent approaches. Open data sharing may be almost as acceptable to participants as controlled data sharing. Some socio-demographic groups differ in their willingness to participate in biobank research.

Peacock S, Reddy A, Leveille SG, Walker J, Payne TH, Oster NV, Elmore JG

Patient portals and personal health information online: perception, access, and use by US adults

J Am Med Inform Assoc 2017 Apr 1;24(e1):e173-e177

Providing patient online record access has been described as fundamental to patient empowerment. Little is known about the effects of the patient-provider relationship on consumer health information technology acceptance and use. To date, progress has been limited in part by professional resistance and concerns about security and privacy. But research has also found sex, race, and age disparities among patients accessing online personal health information (PHI). The primary objective of this study was to evaluate perspectives and patterns of technology use according to demographic characteristics. Authors used the Health Information National Trends Survey (HINTS) to query participants about their demographic characteristics and their views on the importance of having access to their medical records online, whether the access was offered by a health care provider or online via a patient portal. Of the 3,492 survey participants responding to the three primary online PHI questions, a majority (92%) indicated that they felt access to their PHI online was very or somewhat important; just over a third (34%) reported being offered electronic access to their PHI by their health care provider. Less than a third (28%) reported accessing their own PHI online through a secure website or phone application. Respondents who accessed their own PHI online were significantly more likely to report being offered access by their health care provider (P<.001). Regarding demographic characteristics, there were no differences across race or ethnicity in reported the importance of online access (P=.59 and .67, respectively). However, there were significant differences across race and ethnicity in terms of who was offered access by their health care provider (P=.006 and <.001, respectively) and who accessed their PHI online (P=.041 and <.001, respectively). The authors found that individuals who are older, in poor health condition, poorly educated, and members of ethnic or racial minority groups were less likely to be offered online access or to use a portal access. Just one third of respondents indicated that their health care provider offered them access to their records. Any benefits associated with access to patient portals will be less likely to accrue if not offered and used. Of concern is the finding that health care providers offered access in an inconsistent manner, significantly less often to black and Hispanic individuals than to white and non-Hispanic individuals. Authors conclude that to reduce what appears to be typically defined as the digital divide, health care providers may be key factors affecting current patient electronic access patterns. Encouraging physicians and other health care providers to openly discuss this technology and promote access is vital to ensuring that patients both use and benefit from accessing their PHI online.

Walker DM, Johnson T, Ford EW, Huerta TR

Trust Me, I'm a Doctor: Examining Changes in How Privacy Concerns Affect Patient Withholding Behavior

J Med Internet Res 2017 Jan 4;19(1):e2

Health information technology (HIT) can provide clinicians with more complete patient records at the point of care, enabling better clinical decision-making, facilitating improved care coordination, and insuring patient safety as people move throughout the health care system. HIT can also serve as a tool to enable better patient-provider communication, for example through secure messaging, leading to more patient-centred care. Despite these potential benefits, recent high-profile, EHR security breaches reported in the media make patients wary of this shift to the digital format. This study examined changes in the influence of privacy and secu-

rity concerns on Personal Health Information (PHI) withholding behaviour between 2 time points (2011 and 2014). It was based on the Health Information National Trends Survey (HINTS) which is administered as repeat cross-sections by the National Cancer Institute to a national sample of non-institutionalized adults and gathers information regarding attitudes and perceptions about health information access and use. A prepaid incentive was sent at the first mailing, and multiple follow-ups were sent to recipients in order to maximize the response rate. The total number of respondents in the 2011 and 2014 surveys were 3,959 and 3,677, respectively. For the dependent variable (primary outcome), the HINTS survey asked whether the respondent had "ever kept information from (their) health care provider because (they) were concerned about the privacy and security of (their) medical record" (yes, no). The independent variables were the answer (not at all concerned or confident, somewhat concerned or confident, or very concerned or confident) to the following four questions about privacy and security: do respondents have concerns about unauthorized access to their medical information when it is transferred electronically between providers; do respondents have concerns about unauthorized access to their medical information when it is faxed between health care providers; do they feel confident that safeguards are in place to protect their medical information from unauthorized access; and do they feel confident that they had a say in the collection, use, and sharing of their medical information. Overall, 2,217 respondents from 2011 had complete information and were included in the analytic sample, and 2,176 respondents from 2014 were included. Regarding the dependent variable of interest (whether the respondent had ever withheld any PHI from a medical provider out of privacy or security concerns), no difference was observed between years: in 2011, 14.79% (328/2217) of respondents reported this behavior, whereas in 2014, 14.93% (325/2176) of respondents reported withholding information from their provider out of privacy concerns. The analysis also revealed no changes between 2011 and 2014 in the association of privacy and security attitudes on withholding behaviour. Lastly, there was no effect on respondent confidence that they had some control over their medical information on withholding behavior in either year, and no difference was found between the two years. Overall, the analysis suggests that in spite of the existence of security and privacy concerns, focusing resources on the delivery of high-quality care may be an effective strategy to foster patient trust. Patients may perceive quality as an indicator of a provider's carefulness with their medical information.