

Through Patients' Eyes: Regulation, Technology, Privacy, and the Future

Carolyn Petersen

Mayo Clinic, Rochester, Minnesota, United States

Summary

Privacy is commonly regarded as a regulatory requirement achieved via technical and organizational management practices. Those working in the field of informatics often play a role in privacy preservation as a result of their expertise in information technology, workflow analysis, implementation science, or related skills. Viewing privacy from the perspective of patients whose protected health information is at risk broadens the considerations to include the perceived duality of privacy; the existence of privacy within a context unique to each patient; the competing needs inherent within privacy management; the need for particular consideration when data are shared; and the need for patients to control health information in a global setting. With precision medicine, artificial intelligence, and other treatment innovations on the horizon, health care professionals need to think more broadly about how to preserve privacy in a health care environment driven by data sharing. Patient-reported privacy preferences, privacy portability, and greater transparency around privacy-preserving functionalities are potential strategies for ensuring that privacy regulations are met and privacy is preserved.

Keywords

Patient data privacy, self-disclosure, patient-centered care, eHealth, information dissemination

Yearb Med Inform 2018;10-5

<http://dx.doi.org/10.1055/s-0038-1641193>

Introduction

The promise of new technologies, including those intended to improve quality of life for citizens and patients, is a constant theme in health care. Access to information within electronic health records, the ability to incorporate patient-reported outcomes and patient-generated health data into the medical record, mobile health applications, and other functionalities are among the options of which patients are encouraged to avail themselves. New technologies, new ways to create and use health data, and new opportunities for health management have become the organizing principles by which patients and their care teams are expected to live.

As exciting as new technologies can be, they also bring new challenges, including obstacles related to appropriate management of data. The proliferation of new data sources and new data, the desire to make the most and best possible uses of data, and the lack of broadly applicable, implemented data management tools and strategies set up both data users and patients for unexpected situations, unexplained needs, and unfulfilled expectations. Informaticians aspire to make clear what is murky, but being human, struggle to succeed.

In health care, stakeholders largely regard privacy from the viewpoints of legal and regulatory mandates [1, 2]. Statutes are analyzed, requirements are identified, technology meeting requirements is developed, and systems that support and document compliance are implemented. In informatics, privacy is regarded from a technical perspective, as a problem to be solved within technology- and/or workflow-based frameworks [3]. As in health care, requirements are analyzed, technology meeting

requirements is developed, and systems that support and document compliance are implemented. Although biomedical informaticians, physicians, other health care providers, and others have a role to play in issues related to privacy, they don't ordinarily play a significant role in the design of systems that support privacy, at least while maintaining an active clinical practice.

For patients, however, legal and regulatory mandates, clinical workflows, and technology implementations are conceptual, and sometimes irrelevant to day-to-day health, quality of life, and life planning. Although regulations and technical requirements underpin technologies that patients may be required to use when engaging health care providers, in and of themselves regulations and technology have little to do with what patients regard as important. At the same time, patients' desire to exercise control over their health information is evident [4]. This commentary considers the current understanding of privacy and relevant challenges from the patient perspective and offers potential approaches for addressing patient concerns while meeting regulatory and technical requirements.

Privacy Perceptions of Patients

Some observation about privacy from a patient perspective:

1. Patients experience privacy in multiple forms.

The term "privacy" appears in innumerable statutes, regulations, requirements, specifications, and policies as if it were a single concept. In daily life, however,

patients experience privacy as a duality: the privacy of populations and the privacy of individuals. When patients go to the clinic for influenza treatment, the fact that their case will be reported as a matter of public health surveillance does little to deter them from seeking care because they know they will be reported as one of hundreds, if not thousands. The expectation of privacy arises from the perception of safety in numbers, i.e., anonymity among the large number of reported cases.

When patients seek care for conditions not subject to public health reporting, they expect that their privacy will be protected through provider compliance with government regulations and the use of technology (e.g., firewalls and encryption) that protects data in storage and during transmission [5]. Patients also expect that providers will exercise judgment when sharing information with other members of the care team, keeping confidential the information that needs not to be shared in the course of treatment or research uses the patients have approved [6]. Trust that providers and health care organizations will act in accordance with privacy regulations is a key element in patients' relationships with the health care system.

The increasing availability of Big Data and use of artificial intelligence, genomic sequencing, computational biology, and predictive analytics may stimulate additional forms of privacy. For example, patients diagnosed with a particular condition may find themselves to be unexpected and/or unintended members of disease-focused communities whose protected health information (PHI) is subjected to additional sharing and analysis. Or, legislators may define protections for PHI created in social media, resulting in classification of user subgroups. Such situations may by design or practice create experiences of privacy somewhere between privacy of populations and privacy of the individual.

2. Privacy occurs within a context unique to each patient.

Part of what makes privacy protection so challenging is the varying nature of what information patients want protected. What one individual seeks to protect another may disclose freely, for example through social

media, public commentary, or in employment applications. Much of this preference about disclosure is based in underlying needs, such as the desire to protect family and the need to remain employable and insurable.

Informaticians face the challenge of providing privacy to and maintaining privacy of patients whose circumstances, and thus privacy preferences, vary widely:

- *Age.* Older adults, who are less likely to seek educational opportunities, employment, home mortgages, life insurance, or other things that require passing a health exam may be less concerned about loss of privacy than younger adults, who must avoid discrimination based on their health. Nondiscrimination laws may not provide protection for individuals in all situations [7];
- *Socioeconomic status.* Wealthier patients may have access to more advanced privacy-preserving technology and strategies (e.g., turning off personal WiFi when not in use) and may have the education needed to take advantage of opportunities that others cannot [8];
- *Education and digital expertise.* Patients who are better able to understand privacy protection regulations and manage privacy preferences in digital tools may be less concerned about the loss of privacy than those who lack the knowledge, skills, and tools to manage the use of such options [9];
- *Health status.* People who are healthy have relatively less PHI and no need to benefit from information shared by others, so they may see little value in sharing their information. Patients who have one or more conditions and seek new medical knowledge or improved interpretation of existing knowledge to better manage their health may be more open to the risk of loss of privacy because they have a greater need for the potential benefits of data sharing. Furthermore, their declining health may require them to accept loss of privacy as a requirement of seeking medical care, as happens when a person entering a clinical trial must submit to genetic or other testing as a condition of enrollment in the trial. In addition, patients who have relatively mild or non-life-threatening forms of

illness may see sharing information about their condition as a loss of privacy, while those with more serious or advanced conditions may be more comfortable sharing PHI because they have less to lose (e.g., employment-based income or independence) from data sharing;

- *Acute vs. chronic care needs.* Patients who have episodic health issues that aren't likely to affect their future health care needs may be more inclined to view information disclosure as loss of privacy. Those who have chronic health needs may find disclosure of PHI helpful, or even necessary, to ensure they receive the right care at the right time in the right setting;
- *Availability of genetic information.* Because genetic information can be used to predict the likelihood of experiencing some conditions, patients who had genetic testing and/or their family members may have particular concerns about avoiding loss of privacy, even when they have not experienced signs and symptoms of conditions for which they are at higher risk [10];
- *Insurance type and status.* Patients with public insurance and those insured by private companies that have experienced data breaches may be more concerned about the risk of loss of privacy than others who have not been so affected. Patients who receive coverage and care through special programs, such as the US Veterans Administration, also may be sensitized to the privacy loss that may occur following data breaches [11];
- *Use of sensors and tracking devices.* Sensors and tracking devices collect not only information that can be used to assess health status, but also other data such as location and purchases. People who don't use or use a limited number of devices and sensors may be less concerned about loss of privacy than those who use more of these devices, since combining data can yield detailed information about daily routines (e.g., when and where one exercises or when one is at home), personal habits (e.g., how often and when one eats or how often and with whom one has sex), and unhealthy practices (e.g., use of non-prescribed medications, smoking, and excessive drinking).

For patients, information disclosure is often a forced event in which medical events compel them to disclose information they would rather not share. For example, clinicians may need to know a breast cancer patient's HER2 status for treatment planning, or that the genetic test results of one individual may reveal something about others in the family that they would rather not know or wish others not to know [12]. Indelicate handling of the information or even an indifferent attitude on the part of those who handle it can be traumatizing, even more than the actual effects of the disclosure. Although health care providers seek to handle PHI in accord with privacy regulations and thereby avoid distressing patients already burdened by health concerns, the potential for health information technology failures makes it impossible to guarantee confidentiality at all times.

3. Privacy exists alongside many competing needs and cannot represent only patients' goals, even when privacy preservation initiatives are patient-centered.

Even as patients focus on their own health concerns, the interaction with other patients in clinical and social support settings exposes them to the broad range of interests, needs, and goals held by other parties to health care (e.g., providers, health insurance companies, medical product manufacturers, government agencies), some of which are at odds. These competing priorities arise from many sources:

- Varying patient interests, needs, and goals;
- Differing patient and provider/health care organization interests, needs, and goals;
- Differing patient and health care system management/payer interests, needs, and goals;
- Variation among standards and best practices across health care systems;
- Varying availability and use of technologies among patients and health care systems, as well as variation in efficacy and value attained from their use.

Currently, most patients' medical records contain retrospective data; as precision medicine comes into broad use, records eventually may include predictive data as well. Patients'

assessment of the risk of privacy loss and the benefits of disclosure will necessarily become more complex and their decisions more complicated as precision medicine comes into broad use [13]. As other parties to health care exert pressure to meet their interests, needs, and goals, patients and their care teams will face a growing challenge in managing and preserving privacy so that patients can feel comfortable seeking care in whatever forms they believe most beneficial without undue fear of exposure.

4. Sharing is caring – as long as you take care of my data.

Data sharing is among the most promoted and promising benefits of the adoption of the digital health environment. The opportunity to aggregate and analyze large quantities of data holds out hope for new opportunities to determine clinical best practices and identify and develop new treatments. The sharing of clinical and research data, however, comes with patient and family expectations and challenges for health care systems. Within health care, the collection and sharing of data for predetermined health-related purposes seem reasonable enough, but the possibility of unapproved or unintended use of such data in conjunction with other health and non-health data sets may result in reluctance to share data [14].

Privacy and confidentiality are important concerns for patients, but don't prevent large numbers of patients from agreeing to share health information [15, 16]. Although data sharing likely is not top of mind when patients enter the health care system, data-related considerations may become more relevant over time as patients gain a more nuanced understanding of their health and what they need to do to maintain it. Experience with health-related firms, such as direct-to-consumer (DTC) genetic testing companies and fitness training ventures, may inform patient views about privacy as much as or more than engagement with the health care system because commercial ventures may be subject to less stringent regulation and can achieve wide exposure through social media.

In addition, patients have expressed willingness to share information and biospecimens for use in research [17, 18]. Although

patients vary widely in their knowledge and understanding of informed consent processes and their rights to manage their data, they do recognize that others may benefit from the secondary use of their information and support data sharing out of altruism [19]. There is a growing belief among researchers that data sharing should be the norm [20], but patients have yet to adopt that view broadly. Firms that offer DTC genetic testing for health or ancestry tracking purposes have failed to measure up to international transparency guidelines for privacy and secondary data use [21]. As such testing comes into greater use, negative experiences may influence patients' willingness to share medical data.

If patients enroll in a clinical trial, their requirements for privacy preservation may broaden, necessitating a system that offers both patients and researchers flexibility. Establishing clear procedures for data use, qualifying researchers prior to sharing data, providing transparency throughout the process, and returning research results to patients have made sharing of self-reported outcomes data attractive to patients despite the potential for unintended exposure of personal information [22]. Anonymization or de-identification of personal information and the control of access to data through legal agreements provide a starting point for managing data to be used in research [23], though these strategies alone will not engender trust in all patients. Practicing transparency to build and maintain trust must be both underlying principle and practice.

To ensure that data sharing remains acceptable to patients, the health care system needs to recognize the importance of including patients in data governance. Most patients are unlikely to want or take a role in the day-to-day management of health information systems, but they are growing aware of the value of and need for patient-friendly data governance [24, 25]. Governance is a complex process involving many technical, legal, and ethical considerations for both health care professionals and patients; involving patients from the beginning can help providers and researchers more fully understand and respond to patients' needs and goals.

The ability to generate and manage growing quantities of health data created through the use of wearable devices, sensors, mobile health apps, and other tools also drives patients' expectations around data sharing. Such devices are providing patients with new opportunities to manage health concerns that have not been well addressed in medical settings (e.g., weight management) and facilitate quality-of-life improvements in patients with a range of unmet needs, such as long-term cancer survivors [26]. Patients who use self-tracking devices report greater interest in sharing data when they perceive a study to be interesting, receive compensation for sharing data, or can avoid sharing data for commercial ventures [27]. Meeting these objectives will, in many health care environments, necessitate greater involvement of patients at multiple levels. Patients who proactively manage their health want to proactively manage the data generated by the devices they use and expect the health system to make this possible [28].

5. Privacy is global. Data created in one place must follow patients, but never go where patients have not agreed it should go. Even when patients don't travel outside their home country, PHI in their health record or patient-generated health data that they have created can be shared across physical borders. The widespread implementation of electronic health records and growing exchange of health data make it increasingly possible for patients to receive coordinated care, but such opportunity comes with a greater likelihood of data travel to unintended places. This risk will grow, as true interoperability between systems becomes a reality.

As with data, technology has no borders. Large-scale, integrated systems incorporating medical records, clinical decision support, computerized physician order entry, and other functionality may seem far removed from low- and middle-income countries, but the use of mobile health (mHealth), text messaging, and interactive voice response applications in these countries [29-32] shows that digital health not only exists but also thrives in environments that, in other ways, may be resource-limited.

Variations in laws, regulations, and standards across physical borders will become a more pressing issue due to greater patient mobility and changing trends in immigration and movement among refugees and displaced persons. Nonetheless, privacy must be protected across borders even in the absence of electronic data borders.

Next Steps for Informaticians

Historically, health care as a community has focused on the legal and regulatory aspects of privacy and worked to implement compliance-focused technical strategies. Going forward, the injection of practice-changing innovations such as artificial intelligence and genomic sequencing at a large scale offers an opportunity to redesign the collective approach to privacy by starting with user interests, needs, and goals. Patient perceptions provide a starting point from which to envision privacy-preserving approaches of the future.

Patient-reported privacy preferences. The ways in which patients experience privacy are likely to increase in the future as innovations in health care come into widespread use. Patient-reported outcomes (PROs) measures have been developed to record quality of life indicators that are of interest to patients enrolled in clinical trials, such as investigational drug side effects, fatigue, and other parameters of patient experience [33]. The success of PROs in capturing patients' lived experience during trials spurred a movement to incorporate PROs into clinical care, which is gaining momentum within oncology [34] and more broadly [35, 36]. Using this conceptual framework, health information system developers could develop an array of patient-reported privacy preferences (PRPPs) that captures needs, goals, and attitudes affecting the use of PHI. PRPPs could be used in clinical, research, social, wellness, and other settings in which protected health information is collected or generated. Standardizing PRPPs would ensure that privacy settings remained consistent across care settings, thereby reducing the likelihood of confusion at entry and

boosting patient confidence and comfort. Designing PRPPs as measures in the format of published, validated PROs would ensure that PRPPs are suitable for use within the wide range of electronic health records and applications that have been deployed. Over time, de-identified preference data could be analyzed to help designers better understand patients' underlying motivations with regard to privacy and design more nuanced PRPPs and tools to better capture patients' preferences.

Design supporting portability of privacy. With regard to privacy, the flow of data across borders raises two challenges: how to keep data moving with people as individuals travel or relocate, and how to prevent data from moving when patients have expressed the preference that data should not be sent elsewhere. To date, systems design has focused on health information exchange and achievement of interoperability, which remain significant challenges given the prevalence of customized systems implementation in the absence of consistent use of agreed-upon standards. Though much work remains to achieve true interoperability, it is not too early to think about how privacy can be represented within systems for travel with the PHI to which the privacy directives apply. Design in parallel of privacy management and medical information transmission may offer the most expeditious opportunity to achieve privacy portability.

Greater transparency about de-identification and anonymity. Because patients often experience privacy management as a simplified process, for example signing a waiver to release PHI to other care providers or payers, patients often have little practical understanding of how data themselves contribute to loss of privacy. Patients who have frequent involvement with the health care system may have heard of data de-identification, but may not understand enough specifics to realize that some health attributes (e.g., a history of a rare condition, an uncommon genomic sequence) or combinations of attributes may be uncommon enough to allow re-identification of the individual with whom the features are associated [37, 38]. To maintain patient trust and support beneficial patient-provider

relationships, health information system developers could facilitate greater transparency about de-identification, preservation of anonymity, and strategies the health care system uses to prevent loss of privacy. Development of models that predict the scenarios under which individuals can be identified despite correct use of privacy-preserving measures could help health care systems more accurately inform patients about the types of traits and circumstances that make re-identification more likely so that patients can better understand what to expect.

Furthermore, educating patients about the action of privacy-preserving measures can help patients to make more informed decisions about the use of consumer health technologies (e.g., mHealth apps, activity tracking devices) and social media. Though mHealth and social media are used widely worldwide, many users are unaware of the types of personal data collected, the extent of data use by application developers and third parties, the risks to privacy that accompany the use of these technologies, and tactics to reduce the likelihood of unintended privacy loss [39-41]. Given the rising use of devices that create person-generated health data, patient education about privacy protection may be one of the most patient-centered efforts undertaken by health care systems.

Conclusion

Informaticians are accustomed to viewing privacy through legal, regulatory, and technology lenses and working to implement technical strategies. To support coming innovations in health care treatment and technologies, it is necessary to view privacy through the eyes of patients, designing and implementing technologies for their needs and goals as well as those of health care systems. Patients' experience of privacy includes dimensions beyond those typically engaged in managing compliance with privacy regulations, and as a result patients may be inadequately served by current approaches to privacy management. Informaticians are well-positioned to bring together the legal, technical, organizational, consumer health,

and educational skills needed to not only implement known privacy-preserving technologies, but also use patient perspective to design and develop approaches that address patients' interests, needs, and goals. Fulfilling patient goals and needs while also meeting the responsibilities of other health care system parties remains a challenge that may be addressed only through the development of new approaches such as patient-reported privacy preferences, privacy portability technology, and heightened transparency with patients.

References

1. Anthony DL, Stablein T. Privacy in practice: professional discourse about information control in health care. *J Health Organ Manag* 2016;30(2):207-26.
2. Mackenzie IS, Manray BJ, McDonnell PG, Wei L, MacDonald TM. Managing security and privacy concerns over data storage in healthcare research. *Pharmacoepidemiol Drug Saf* 2011;20(8):885-93.
3. Lee LM. Ethics and subsequent use of electronic health record data. *J Biomed Inform* 2017;71:143-6.
4. Caine K, Hanania R. Patients want granular privacy control over health information in electronic medical records. *J Am Med Inform Assoc* 2013;20(1):7-15.
5. Cochran GL, Lander L, Morien M, Lomelin DE, Brittin J, Reker C, et al. Consumer opinions of health information exchange, e-prescribing, and personal health records. *Perspect Health Inf Manag* 2015;12:1e.
6. Dimitropoulos L, Patel V, Scheffler SA, Posnack S. Public attitudes toward health information exchange: perceived benefits and concerns. *Am J Manag Care* 2011;17(12 Spec No.):SP111-6.
7. Genetic discrimination lawsuit raises broader concerns about testing, privacy: Case involves middle school student impacted by results of genetic screening test as newborn. *Am J Med Genet A* 2016;170A(5):1111-2.
8. Gilman ME. The class differential in privacy law. *Brooklyn Law Rev* 2012;77(4):389-1445.
9. Pasquale F. Redefining health privacy: the importance of information policy. *Houston J Health Law Policy* 2014;14:95-128.
10. Deverka PA, Majumder MA, Villanueva AG, Anderson M, Bakker AC, Bardill J, et al. Creating a data resource: what will it take to build a medical information commons? *Genome Med* 2017;9(1):84.
11. Lee C. Veterans angered by file scandal. *Washington Post*. 24 May 2006. Available at: <http://www.washingtonpost.com/wp-dyn/content/article/2006/05/23/AR2006052301603.html> (Accessed 12/2/2017).
12. Brothers KB, East KM, Kelley WV, Wright ME, Westbrook MJ, Rich CA, et al. Eliciting preferences on secondary findings: the Preferences Instrument for Genomic Secondary Results. *Genet Med* 2017;19(3):337-44.
13. Kulynych J, Greely HT. Clinical genomics, big data, and electronic medical records: reconciling patient rights with research when privacy and science collide. *J Law Biosci* 2017;4(1):94-132.
14. O'Doherty KC, Christofides E, Yen J, Bentzen HB, Burke W, Hallowell N, et al. If you build it, they will come: unintended future uses of organized health data collections. *BMC Med Ethics* 2016;17:54.
15. Kim KK, Joseph JG, Ohno-Machado L. Comparison of consumers' views on electronic data sharing for healthcare and research. *J Am Med Inform Assoc* 2015;22:821-30.
16. Weitzman ER, Keleman S, Kaci L, Mandl KD. Willingness to share personal health record data for care improvement and public health: a survey of experienced personal health record users. *BMC Med Inform Decis Mak* 2012;12:39.
17. Page SA, Manhas KP, Muruve DA. A survey of patient perspectives on the research use of health information and biospecimens. *BMC Med Ethics* 2016;17:48.
18. Aitken M, de St. Jorre J, Pagliari C, Jepson R, Cunningham-Burley S. Public responses to the sharing and linkage of health data for research purposes: a systematic review and thematic synthesis of qualitative studies. *BMC Med Ethics* 2016;17:73.
19. Spencer K, Sanders C, Whitley EA, Lund D, Kaye J, Dixon WG. Patient perspectives on sharing anonymized personal health data using a digital system for dynamic consent and research feedback: a qualitative study. *J Med Internet Res* 2016;8(4):e66.
20. Krumholz HM. Why data sharing should be the expected norm. *BMJ* 2015;350:h599.
21. Laestadius LI, Rich JR, Auer PL. All your data (effectively) belong to us: data practices among direct-to-consumer genetic testing firms. *Genet Med* 2017;19(5):513-20.
22. Wilbanks J, Friend SH. First, design for data sharing. *Nat Biotechnol* 2016;34(4):377-79.
23. Tucker K, Branson J, Dilleen M, Hollis S, Loughlin P, Nixon MJ, et al. Protecting patient privacy when sharing patient-level data from clinical trials. *BMC Med Res Methodol* 2016;16(Suppl 1):77.
24. Petersen C. The future of patient engagement in the governance of shared data. *EGEMS*. 2016;4(2):1214.
25. Agaku IT, Adisa AO, Ayo-Yusuf OA, Connolly GN. Concern about security and privacy, and perceived control over collection and use of health information are related to withholding of health information from healthcare providers. *J Am Med Inform Assoc* 2014;21:374-8.
26. Petersen C. Patient-generated health data: a pathway to enhanced long-term cancer survivorship. *J Am Med Inform Assoc* 2016;23:456-61.
27. Bietz MJ, Bloss CS, Calvert S, Godino JG, Gregory J, Claffey MP, et al. Opportunities and challenges in the use of personal health data for health research. *J Am Med Inform Assoc* 2016;23:e42-8.
28. Nash IS. It's my heart: why not my data? *Circulation* 2018;137(1):4-6.
29. Hoque R, Sorwar G. Understanding factors influ-

- encing the adoption of mHealth by the elderly: an extension of the UTAUT model. *Int J Med Inform* 2017;101:75-84.
30. Sondaal SF, Browne JL, Amoakoh-Coleman M, Borgstein A, Miltenburg AS, Verwijs M, Klipstein-Grobusch K. Assessing the effect of mHealth interventions in improving maternal and neonatal care in low- and middle-income countries: a systematic review. *PLoS One* 2016;11(5):e0154664.
 31. Brinkel J, Dako-Gyeke P, Krämer A, May J, Fobil JN. An investigation of users' attitudes, requirements and willingness to use mobile phone-based interactive voice response systems for seeking healthcare in Ghana: a qualitative study. *Public Health* 2017;144:125-33.
 32. Chib A, van Velthoven MH, Car J. mHealth adoption in low-resource environments: a review of the use of mobile healthcare in developing countries. *J Health Commun* 2015;20(1):4-34.
 33. Dueck AC, Mendoza TR, Mitchell SA, Reeve BB, Castro KM, Rogak LJ, et al. Validity and reliability of the US National Cancer Institute's patient-reported outcomes version of the common terminology criteria for adverse events (PRO-CTCAE). *JAMA Oncol* 2015;1(8):1051-9.
 34. Basch E, Deal AM, Dueck AC, Scher HI, Kris MG, Hudis C, Schrag D. Overall survival results of a trial assessing patient-reported outcomes for symptom monitoring during routine cancer treatment. *JAMA* 2017;318(2):197-8.
 35. Harle CA, Listhaus A, Covarrubias CM, Schmidt SOF, Macket S, Carek PJ, et al. Overcoming barriers to implementing patient-reported outcomes in an electronic health record: a case report. *J Am Med Inform Assoc* 2016;23(1):74-9.
 36. Basch E, Snyder C. Overcoming barriers to integrating patient-reported outcomes in clinical practice and electronic health records. *Ann Oncol* 2017;28(10):2332-3.
 37. Lippert C, Sabatini R, Maher MC, Kang EY, Lee S, Arkan O, et al. Identification of individuals by trait prediction using whole-genome sequencing data. *Proc Natl Acad Sci U S A* 2017;114(38):10166-71.
 38. Kushida CA, Nichols DA, Jadrnicek R, Miller R, Walsh JK, Griffin K. Strategies for de-identification and anonymization of electronic health record data for use in multicenter research studies. *Med Care* 2012;50 Suppl:S82-101.
 39. Müthing J, Jäschke T, Friedrich CM. Client-focused security assessment of mHealth apps and recommended practices to prevent or mitigate transport security issues. *JMIR Mhealth Uhealth* 2017;5(10):e147.
 40. Dehling T, Gao F, Schneider S, Sunyaev A. Exploring the far side of mobile health: information security and privacy of mobile health apps on iOS and Android. *JMIR Mhealth Uhealth* 2015;3(1):e8.
 41. Martínez-Pérez B, de la Torre-Díez I, López-Coronado M. Privacy and security in mobile health apps: a review and recommendations. *J Med Syst* 2015;39(1):181.

Correspondence to:

Carolyn Petersen, MBI, MS
 Mayo Clinic
 Rochester, Minnesota, USA
 E-mail: petersen.carolyn@mayo.edu