Virtual Mentor
American Medical Association Journal of Ethics
December 2014, Volume 16, Number 12: 981-985.

IN THE LITERATURE

Privacy and Security Concerns in Telehealth

Timothy M. Hale, PhD, and Joseph C. Kvedar, MD

Hall JL, McGraw D. For telehealth to succeed, privacy and security risks must be identified and addressed. *Health Aff (Millwood)*. 2014;33(2):216-221.

Innovative connected health technologies offer a promising solution to many of the challenges facing health care delivery in the United States. Connected health refers to a wide range of care delivery models that utilize communications technologies (sometimes referred to as telehealth and telemedicine) to help patients manage their conditions through improved self-care and to extend clinical care outside of traditional settings [1]. Health care systems that combine patient-reported information and objective data from telehealth devices and sensors can be used to create patient-centered, personalized health interventions. Although these new technologies promise to improve the quality of care, reduce costs, and increase patient satisfaction, they raise a number of ethical issues.

Hall and McGraw argue that there are significant privacy and security risks in telehealth systems that can adversely affect patients' and clinicians' level of trust and willingness to adopt and use the system [2]. Noting that current regulations do not provide sufficient guidance for developers or protection for users, the authors recommend that a single federal agency, the Federal Trade Commission (FTC), coordinate the creation and enforcement of comprehensive privacy and security standards. In what follows, we summarize Hall and McGraw's key points and then discuss their implications based on our experience in creating, evaluating, and implementing telehealth systems.

Hall and McGraw begin by describing the risks that telehealth systems pose to the privacy and security of patients' health information. Privacy risks involve a lack of control over the collection, use, and sharing of data. For example, home telehealth devices and sensors designed to detect falls may collect and transmit information on activities in the household that a patient wishes to keep private, such as substance abuse or that the house is unoccupied at particular time. Smartphone apps may share sensitive data—such as sensor data on location—with advertisers and other third parties in ways not anticipated by users. The primary security risk is that of unauthorized access to data during collection, transmission, or storage. Any transfer offers the potential for a security breach. The authors argue that, despite efforts to create secure devices and apps, many contain serious flaws, and hackers and malware pose an increasing threat to the security of telehealth systems.

Hall and McGraw explain that existing regulations are insufficient to provide strong privacy and risk protections for users. Currently, the Health Insurance Portability and Accounting Act (HIPAA) contains the primary set of regulations that guide the privacy and security of health information. HIPAA requires that identifiable health information be encrypted so that only those authorized to read it can do so. HIPAA, however, applies only to “covered entities”—health care providers and insurers—not to patients. The Food and Drug Administration (FDA) regulates medical devices but not consumer-facing devices and apps, focusing on technical issues related to the security and integrity of information. In this way, the FDA ensures patient safety but not patient privacy; hence, Hall and McGraw propose that Congress authorize a single federal agency, the Federal Trade Commission (FTC), to create and enforce telehealth privacy and security regulations.

The FTC has expertise in privacy and technical issues related to security, in creating and enforcing consumer protection laws, and in supporting innovation. The authors recommend that the FTC enlist stakeholders and manufacturers in creating voluntary codes of conduct for protecting privacy and security and provide a “safe harbor” or protection from legal action to entities that operate under these codes. If no agreement were reached on voluntary standards, the FTC would exercise its authority to create and enforce federal regulations. Hall and McGraw conclude that giving the FTC this two-part authority is the best option for creating comprehensive privacy and security standards that will ensure telehealth systems are trusted and adopted [2].

Discussion

Hall and McGraw provide a useful description of and suggested resolution for the privacy and security challenges facing the development of successful telehealth systems, but there are several caveats to accepting the authors’ recommendation for an FTC solution.

First, there is the possibility that establishing voluntary standards or new federal regulations aimed at telehealth systems may not significantly improve users’ level of trust, even if such steps improve privacy and security protections. Increased reporting of security breaches, which are almost a daily occurrence, may have contributed to a general sense of distrust in electronic transmission and storage of personal information that may not diminish with regulations directed solely at telehealth. For example, as this paper was being written, a cyber-attack was launched with the “Backoff” malware—first used in a widely publicized 2013 theft of information from Target—to steal consumers’ payment card information from as many as 1,000 businesses [3]. What may be needed is a comprehensive set of privacy and security standards and regulations not exclusively for health data but for all consumer data that is collected, stored, and shared electronically [4].

Second, many people remain interested in using telehealth systems despite their concerns about the privacy and security of their health information [5]. A California Health Care Foundation survey in 2010 found that, although 66 percent of adults thought that there was a need to address concerns about the privacy of their personal medical information [6], they agreed with the statement that “we should not let privacy concerns stop us from learning how technology can improve our health care” [7]. In addition, more than half of the adults surveyed were interested in using technology to monitor their health and almost half were interested in using telehealth devices to send health information to their doctors [6].

In fact, people may be more willing to accept privacy risks when they perceive that the health benefits of using telehealth systems outweigh the risks involved in sharing their information. For example, a study of focus groups on technology’s future role in improving health care management found that healthy participants were more concerned about privacy than participants with chronic conditions [8]. In general, for most people, the convenience of rapid access to information and communication with clinicians outweighed privacy concerns. Another example of a privacy trade-off comes from a study we are conducting at the Center for Connected Health involving asthmatic teens’ use of Facebook to share their experiences living with asthma and to improve self-management and medication adherence. To ensure some level of privacy in sharing identifiable health information, we are using a private Facebook group accessible only to study participants. Despite the potential privacy risks, legal guardians give permission for teens to participate, and teens are active in the group (unpublished data, study in progress).

A third caveat is that, despite the potential for telehealth systems to automate some tasks and deliver care outside of the clinic, patients’ trust in their clinicians will play an important role in their adoption of telehealth technologies. Such trust is built on good patient-physician communication [9] and contributes to improved treatment adherence and continuity of care [10]. Physicians should discuss the benefits and risks of using telehealth and other technologies as part of a patient-centered care plan [11]. Due to the rapid pace of innovation it is unlikely that voluntary codes and regulatory agencies can provide guidance on all situations and new technologies [12]. Therefore, physicians will need to stay informed of their institutions’ privacy and security policies and discuss these with patients as part of their ethical obligation to ensure patient-physician confidentiality.

Finally, to encourage patients to adopt and use telehealth systems, clinicians must do so first. At the Center for Connected Health, we have seen that clinicians’ use of telehealth is a key factor in telehealth systems’ success in improving clinical outcomes. For example, among diabetic patients who were using a text messaging program that delivered personalized coaching to promote physical activity and blood glucose control, those patients whose physicians did not log in to view their results were more likely to stop using the program than patients whose doctors did log in to view the results [13]. Therefore, the integration of telehealth systems into clinicians’ workflows and standard of care will be essential to patient adoption and sustained use of telehealth systems and, ultimately, to their success.

Conclusion

Concerns about the privacy and security of telehealth systems may adversely affect people's trust in telehealth and threaten the ability of these systems to improve the accessibility, quality, and effectiveness of health care. More comprehensive standards and regulations may be needed to ensure strong privacy and security protections not only for telehealth but also for all electronic consumer information. But many people, especially the chronically ill, believe the benefits of using telehealth systems outweigh the risks. Physicians can contribute to the success of telehealth by creating patient-centered care plans that effectively use telehealth tools and make sure patients are aware of potential privacy and security risks.

References

1. Kvedar J, Coye MJ, Everett W. Connected health: a review of technologies and strategies to improve patient care with telemedicine and telehealth. *Health Aff (Millwood)*. 2014;33(2):194-199.
2. Hall JL, McGraw D. For telehealth to succeed, privacy and security risks must be identified and addressed. *Health Aff (Millwood)*. 2014;33(2):216-221.
3. Perlroth N. US finds "Backoff" hacker tool is widespread. *New York Times*. August 22, 2014. http://bits.blogs.nytimes.com/2014/08/22/secret-service-warns-1000-businesses-on-hack-that-affected-target. Accessed October 14, 2014.
4. King NJ, Raja VT. Protecting the privacy and security of sensitive customer data in the cloud. *Comput Law Secur Rev*. 2012;28(3):308-319.
5. Vodicka E, Mejilla R, Leveille SG, et al. Online access to doctors' notes: patient concerns about privacy. *J Med Internet Res*. 2013;15(9):e208.
6. California HealthCare Foundation. Consumers and health information technology: a national survey. Oakland, CA: California HealthCare Foundation; 2010. http://www.chcf.org/~/media/MEDIA%20LIBRARY%20Files/PDF/C/PDF%20ConsumersHealthInfoTechnologyNationalSurvey.pdf. Accessed October 14, 2014.
7. California HealthCare Foundation, 26.
8. Walker J, Ahern DK, Le LX, Delbanco T. Insights for internists: "I want the computer to know who I am." *J Gen Intern Med*. 2009;24(6):727-732.
9. Fiscella K, Meldrum S, Franks P, et al. Patient trust: is it related to patient-centered behavior of primary care physicians? *Med Care*. 2004;42(11):1049-1055.
10. Thom DH, Hall MA, Pawlson LG. Measuring patients' trust in physicians when assessing quality of care. *Health Aff (Millwood)*. 2004;23(4):124-132.
11. Fleming DA, Edison KE, Pak H. Telehealth ethics. *Telemed J E Health*. 2009;15(8):797-803.
12. Wang CJ, Huang DJ. The HIPAA conundrum in the era of mobile health and communications. *JAMA*. 2013;310(11):1121-1122.
13. Jethwani K, Ling E, Mohammed M, Myint-U K, Pelletier A, Kvedar JC. Diabetes connect: an evaluation of patient adoption and engagement in a

web-based remote glucose monitoring program. *J Diabetes Sci Technol*. 2012;6(6):1328-1336.

Timothy M. Hale, PhD, is a research fellow at the Center for Connected Health and Harvard Medical School in Boston. He received his doctorate in medical sociology from the University of Alabama, Birmingham, in 2011. His work has been published in the *Journals of Gerontology, Journal of Health Communication: International Perspectives, American Behavioral Scientist,* and *Information, Communication and Society*. His current research examines how new information and communication technologies are transforming existing models of health care and emerging digital health lifestyles.

Joseph C. Kvedar, MD, is the founder and director of the Center for Connected Health and associate professor of dermatology at Harvard Medical School in Boston. A frequent lecturer, Dr. Kvedar has authored more than 70 publications on connected health and the application of communications technologies to improve health care. He serves as a board member on the Continua Health Alliance and the Population Health Alliance, was a president and board member of the American Telemedicine Association (ATA), and was a chair of the American Academy of Dermatology (AAD) Telemedicine Task Force. In 2009, Dr. Kvedar was honored with the ATA's Individual Leadership Award for his significant contributions to connected health and telemedicine.

Related in VM

Electronic Health Records: Privacy, Confidentiality, and Security, September 2012

Ethical Dimensions of Meaningful Use Requirements for Electronic Health Records, March 2011

The viewpoints expressed on this site are those of the authors and do not necessarily reflect the views and policies of the AMA.

Copyright 2014 American Medical Association. All rights reserved.