By Joseph L. Hall and Deven McGraw

DOI: 10.1377/hlthaff.2013.0997
HEALTH AFFAIRS 33,
NO. 2 (2014): 216–221

For Telehealth To Succeed, Privacy And Security Risks Must Be Identified And Addressed

Joseph L. Hall (joe@cdt.org) is chief technologist at the Center for Democracy and Technology, in Washington, D.C.

Deven McGraw is director of the Health Privacy Project at the Center for Democracy and Technology.

ABSTRACT **The success of telehealth could be undermined if serious privacy and security risks are not addressed. For example, sensors that are located in a patient's home or that interface with the patient's body to detect safety issues or medical emergencies may inadvertently transmit sensitive information about household activities. Similarly, routine data transmissions from an app or medical device, such as an insulin pump, may be shared with third-party advertisers. Without adequate security and privacy protections for underlying telehealth data and systems, providers and patients will lack trust in the use of telehealth solutions. Although some federal and state guidelines for telehealth security and privacy have been established, many gaps remain. No federal agency currently has authority to enact privacy and security requirements to cover the telehealth ecosystem. This article examines privacy risks and security threats to telehealth applications and summarizes the extent to which technical controls and federal law adequately address these risks. We argue for a comprehensive federal regulatory framework for telehealth, developed and enforced by a single federal entity, the Federal Trade Commission, to bolster trust and fully realize the benefits of telehealth.**

Telehealth involves the use of telecommunication technologies to prevent and treat illness and promote the health of individuals and populations. Although telehealth has particular benefits for rural and underserved populations, it is increasingly recognized for its potential to control costs while providing real-time tools to promote wellness, prevent disease, and enable the home management of chronic conditions.

Telehealth frequently involves bidirectional, digital collection and communication of sensitive health information among health care providers and patients. For a medical device to qualify as a telehealth device, there must be communication of health information from the device over a network. For example, a glucose monitor becomes a telehealth device when it sends readings to a provider or a provider's information system over an information network. Similarly, some generic communications technologies—such as videoconferencing—are frequently used to communicate health care information and thus become telehealth tools in those settings. Telehealth devices include mobile software applications (apps) in addition to hardware. This article focuses on network-enabled telehealth devices where a device collects information from the patient (for example, measuring a function of the body or scanning the environment for safety risks) and then transmits data to a health care provider.

To realize telehealth's full potential, however, patients and providers must trust telehealth systems to keep personal information private and secure. We identify privacy and security risks of telehealth systems, summarize the extent to

which technical controls and current federal laws do—and do not—adequately address those risks, and include recommendations for building and maintaining public trust in telehealth systems through a comprehensive regulatory framework developed and enforced by the Federal Trade Commission (FTC).

Potential Privacy Risks

Privacy risks of telehealth involve a lack of controls or limits on the collection, use, and disclosure of sensitive personal information. Sensors that are located in a patient's home or that interface with the patient's body to detect safety issues or medical emergencies may inadvertently collect sensitive information about household activities. For instance, home sensors intended to detect falls may also transmit information such as interactions with a spouse or religious activity, or indicate when no one is home.

Routine transmissions from a medical device may be collected and stored by the device or app manufacturer, not just the health care provider. A mobile health app may be financed by sharing potentially sensitive data from the app with third-party advertisers that target ads to patients based on app use. Such collection, use, and disclosure of information may be beyond what patients reasonably expect given anticipated uses of the technology. For example, in 2011 the popular fitness device Fitbit inadvertently exposed users' self-reported sexual activity, failing to acknowledge that some forms of physical exertion may be sensitive information.[1]

Patients give consent for having a device implanted or sensors embedded, or for using a health app. However, overreliance on consent too often results in weak privacy protections. Patients frequently do not read or fully understand privacy policies, and consent shifts the burden of privacy protection to the patient, who may not be able to make meaningful privacy choices.[2]

Privacy Controls

Privacy is typically protected by laws or operating policies that implement Fair Information Practice Principles (FIPPs). FIPPs are widely accepted practices, including the ability to access one's own health information and request corrections; limitations on information collection, use, and disclosure; and reasonable opportunities to make choices about one's own health information. Providing people with choices for information sharing is only one of the FIPPs, bolstered by others that require data holders to establish and abide by contextually appropriate limits on data access, use, and disclosure.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is one of several sectoral federal laws designed to implement these principles. Current laws, however, do not adequately cover the telehealth environment, as discussed in later sections. Thus, there is no guaranteed right (and often little capability) for individuals to request copies of information collected by apps or home monitoring devices. Information use and disclosure is largely determined by technology companies, with few (if any) legal limits or meaningful opportunities for individuals to control information flow.[3]

Potential Security Risks

Detailing the security risks and appropriate security controls for telehealth systems involves specifying what kinds of security threats they should protect against. In telehealth delivery models involving provider-to-provider communication, the entities at both ends are typically required by HIPAA to implement appropriate security safeguards, such as authentication and data encryption measures (see "Security Controls" below). However, in telehealth models where one end of the communication ("endpoint") is the patient (for example, an implantable device that sends signals to a physician, or a mobile health app on a patient's cell phone), that endpoint falls outside the controlled and supervised environment of a HIPAA-regulated clinical care setting, magnifying existing privacy and security concerns.

For a typical telehealth system where a provider communicates with a patient, relevant threats include breach of confidentiality during collection of sensitive data or during transmission to the provider's system; unauthorized access to the functionality of supporting devices as well as to data stored on them; and untrusted distribution of software and hardware to the patient. Although we are unaware of direct harm to patients associated with a security flaw in a telehealth system, there have been academic demonstrations of such problems. For instance, certain insulin pumps have been shown to be vulnerable to hacking.[4] There also have been instances where unauthorized software, such as file-sharing software installed by a health care employee, led to a breach of health information and medical identity theft.[5]

Security Controls

A number of existing technical controls can protect against these security risks.[6] Data encryption—where data are electronically "locked"

using complex mathematics and encryption "keys"—can ensure that if an attacker gains access to the raw data, those data will be meaningless. There are various functional types of data encryption: while data are "at rest" (being stored) or "in transit" (being transmitted), and from "end to end" (a type of encryption that does not depend on the state of the data). At-rest and in-transit encryption typically rely on encryption methods provided by operating systems and browsers. These methods are usually external to the telehealth software. With end-to-end encryption, encryption may be directly incorporated into the telehealth application. Encryption of data at rest ensures that when an attacker bypasses access controls, the data are meaningless. Encryption of data in transit guarantees that data are meaningless if a transmission is intercepted. In "end-to-end" encryption, unencrypted information is only ever available at the two endpoints and never between.[7]

With encryption, anyone with the correct key can retrieve meaningful data. Access to the underlying information system, however, can be further controlled using authentication and access control mechanisms, which restrict access to information based on the identity of the person accessing the data or his or her role within an organization.

In addition, medical and consumer devices typically used by patients for telehealth applications can themselves pose serious risks, as the devices contain numerous security flaws and are constantly under attack from threats such as malware.[8] Mobile platforms control this by prohibiting the installation of software that has not been examined and approved.

A final security control for telehealth software and devices involves initially distributing them to patients in a face-to-face setting. This enables the provider to establish the identity of the patient and authenticate the device she or he is using. This way, providers know they are not introducing security risks by accepting data from a potentially unsafe patient device (from a security, not a health risk, standpoint), and patients have some assurance about the quality of the hardware and software, because they interact with an experienced provider to obtain, install, and configure the device.

HIPAA Protections

HIPAA privacy and security regulations provide protections for identifiable health information, but only when it is collected and shared by "covered entities"—health care providers who bill electronically using HIPAA standards, health plans, and health care clearinghouses.[9] When it applies, HIPAA's Privacy Rule establishes limits on the use and disclosure of identifiable health information, and its Security Rule establishes technical, physical, and administrative safeguards to be adopted to protect electronic identifiable health information. For example, encryption of data at rest and in transit is an "addressable implementation specification" under the Security Rule, meaning that HIPAA-covered entities are expected to implement it unless it is not "reasonable and appropriate" to do so.[10] In addition, the regulation states, providers are required to adopt identity management protocols and access controls.

In the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, Congress extended HIPAA to "business associates," entities that "create, receive, maintain, or transmit" identifiable health information to perform a function or service "on behalf of" a covered entity.[11] Whether a vendor of a patient-facing telehealth technology is a HIPAA business associate depends on whose interests are being served by the technology. Relevant questions include the following: Who provides the technology to the patient (for example, is it a direct-to-patient transaction, or is the technology provided by the doctor)? Who benefits from the technology being offered? Who is responsible for the day-to-day operation of the technology (an indication of who is ultimately responsible)? And who controls the information generated by the technology? Mere connectivity between a device and a health care provider does not render the device manufacturer a business associate of that provider.[12]

Other Federal Protections

Given HIPAA's limited applicability to patient-facing telehealth systems,[13] its protections will not apply to information collected by most digital tools provided to patients. Additional federal laws provide some protections, however. In section 13407(f)(2) of the HITECH Act, Congress established breach notification requirements for personal health records. The requirements are overseen by the FTC. Section 13400(11) of the HITECH Act defines a *personal health record* as an electronic record of identifiable information "drawn from multiple sources and…managed, shared, and controlled" by the patient. Some tools of telehealth, such as network-enabled medical devices, would not fit this definition, as they do not draw information from multiple sources and are not typically controlled by the patient. As a result, the HITECH breach notification provisions will not apply.

The FTC also has authority under the Federal

The FDA does not directly address privacy issues but focuses on security to the extent that it affects medical device safety.

Trade Commission Act to prevent, and seek redress for, unfair or deceptive acts or practices.[14] The FTC has used this authority frequently to penalize consumer-facing, for-profit companies for failing to abide by commitments regarding data use made in privacy policies and less frequently to stop unfair practices involving data use and collection.[15] As a result, patients using apps and other telehealth devices must largely rely on company policies regarding uses of data, typically found in a company's privacy policy or the license agreement. These policies are frequently offered to users unilaterally: Accept the terms or don't use the product. Unfortunately, in the case of medical devices, patients often do not have a choice.

The FTC also expects companies to implement reasonable security safeguards and has acted in cases of unfair design, unfair default settings, and unfair data security practices that cause substantial injury to consumers and are not offset by other benefits.[15] Because the FTC does not set detailed requirements for either data privacy or security, protections for telehealth technologies not covered by HIPAA are largely dependent on the technology vendor's discretion.

If a telehealth technology qualifies as a medical device, the Food and Drug Administration (FDA) may also regulate it. The FDA does not directly address privacy issues but focuses on security to the extent that it affects medical device safety. (The FDA regulation of mobile medical apps is discussed in greater detail elsewhere in this issue.)[16] In June 2013 the FDA issued draft guidance on "management of cybersecurity in medical devices,"[17] which urges manufacturers to develop security controls to maintain information "confidentiality, integrity and availability." In August 2013 the FDA finalized guidance regarding radio frequency wireless technology in medical devices.[18] And in September 2013 the FDA issued broad guidance on the regulation of mobile medical apps, clarifying that some types of mobile medical apps will be considered medical devices and regulated by the FDA as such.[19]

Through these guidance documents, the FDA is establishing a federal baseline for security in telehealth, but the FDA's authority has limits. The FDA oversees only technologies it considers to be medical devices and focuses only on security protections designed to ensure safety. It does not focus on privacy safeguards that enforce rules or policies regarding collection, use, and disclosure of potentially sensitive health information.

Building Trust

A comprehensive federal policy framework protecting the privacy and security of information collected by telehealth technologies is needed to safeguard patients and bolster public trust. Such protections should be consistent with HIPAA, to ensure a rational and predictable policy environment, but they also should respond to threats to privacy and security that are more characteristic of patient- and consumer-facing technologies. Specifically, policy should address issues such as deficiencies in security safeguards, reliance by app companies on advertising within the apps, and consumers' lack of access to their information. Such policies should be tailored to address the unique telehealth risks we have identified here. The policies should cover data collection, use, and disclosure, for both the intended purpose of the technology and any secondary data uses, such as for analytics. They should also be flexible enough to support innovation.

There are a number of challenges to crafting such a policy framework. Privacy and security concerns sometimes can conflict with practicality for patients and industry. Privacy and security controls that do not anticipate the needs and preferences of the intended users are less likely to be deployed. For example, only half of iPhone users lock their devices with a passcode, which prompted Apple to integrate a fingerprint reader into newer models of the iPhone to make it easier to lock the device.[20]

This tension between operational practicality on the one hand and privacy and security on the other also exists in other sectors, such as telecommunications and banking. Both the Cable TV Privacy Act of 1984 and the Telecommunications Act of 1996 prevent the disclosure of personal information without consent and also provide some FIPPs-like protections, while balancing the business and operational needs of cable and telecommunications providers by al-

lowing the sharing of personal information if the customer fails to opt out of such sharing.[21,22] In banking, the Fair Credit Reporting Act of 1970 and the Gramm-Leach-Bliley Act of 1999 heavily regulate what credit reporting agencies and financial services companies can do with personal information, providing for conspicuous and regular notice of privacy practices and rights of correction and transparency for consumers. However, these laws also favor an opt-out approach for sharing personal information—allowing data to flow by default to other companies unless the customer specifically opts out.[23,24]

Unfortunately, no federal agency currently has authority to enact privacy and security requirements to cover the telehealth ecosystem. We argue that Congress must establish general standards for data protection in telehealth and vest primary authority for telehealth privacy and security oversight with one federal agency. The Department of Health and Human Services (HHS), with experience in implementing HIPAA and overseeing US health programs, is an obvious candidate. However, no HHS office or agency has experience with the privacy and security risks introduced by consumer-facing commercial technologies, and, as noted above, the FDA's focus is on safety, not privacy. The ideal agency should have a track record of experience on privacy and technical security issues and be nimble and supportive of innovation.

The FTC, with its growing technical expertise and long experience in evaluating the privacy risks of consumer-facing technologies, is the agency within the federal government most equipped to regulate information privacy, including within networked telehealth systems. With respect to telehealth, Congress should give the FTC two-part authority. First, building on the Department of Commerce's 2010 outline for "voluntary enforceable codes of conduct" with respect to consumer privacy,[25] the FTC should facilitate development of voluntary codes of conduct by telehealth manufacturers and other interested stakeholders that include baseline privacy and security protections. Because the telehealth environment is rapidly evolving, involvement of manufacturers and other stakeholders in developing privacy and security codes of conduct is critical. The FTC, under its existing authority to regulate deceptive and unfair practices, can enforce these protections among telehealth manufacturers that commit to adopting them. To induce industry to develop and adopt these codes of conduct, the FTC should provide a safe harbor from enforcement action for those activities governed by the codes. To ensure meaningful protections, safe harbor should be granted only to codes that the FTC deems to be sufficiently consumer protective.

Action by policy makers is needed to ensure a level playing field for companies and a reliable privacy and security policy environment for patients.

If no code of conduct can be agreed upon by a multistakeholder group, the FTC should have the authority to develop its own regulations establishing a basic set of privacy protections and security controls for the telehealth industry. The threat of such regulation should inspire industry participation in a voluntary effort.

In the absence of clear federal policy, states have greater incentives to enact their own protections, hindering the establishment of a consistent, national policy environment. Voluntary adoption of FIPPs-based privacy policies and strong security safeguards can help fill gaps, but they are no substitute for national policies, as industry self-interest too often prevents self-regulation from establishing strong protections.[26] Ultimately, action by policy makers is needed to ensure a level playing field for companies and a reliable privacy and security policy environment for patients.

Conclusion

Telehealth is a rapidly evolving and rich sector of mobile computing and networking that holds clear promise for improving health care. However, serious privacy and security risks could undermine this potential. Congress should authorize federal telehealth privacy and security protections, to both avoid conflicting state-based regulation and assure realization of the benefits of telehealth. We posit that the FTC is the federal agency most suited for regulating this industry. Congress should direct the FTC to facilitate the adoption by telehealth companies of voluntary telehealth security and privacy codes

of conduct, which the FTC can enforce through its existing authority. The agency should be empowered to develop its own regulations if voluntary efforts prove unsuccessful. ■

The authors gratefully acknowledge the support of the Markle Foundation and the California HealthCare Foundation for this work.

NOTES

1 Hill K. Fitbit moves quickly after users' sex stats exposed. Forbes [serial on the Internet]. 2011 Jul 5 [cited 2014 Jan 6]. Available from: http://www.forbes.com/sites/kashmirhill/2011/07/05/fitbit-moves-quickly-after-users-sex-stats-exposed/

2 McGraw D, Dempsey JX, Harris L, Goldman J. Privacy as an enabler, not an impediment: building trust into health information exchange. Health Aff (Millwood). 2009; 28(2):416–27.

3 Dockser Markus A, Weaver C. Heart gadgets test privacy-law limits. Wall Street Journal. 2012 Nov 28.

4 Paul N, Kohno T, Klonoff D. A review of the security of insulin pump infusion systems. J Diabetes Sci Technol. 2011;5(6):1557–62.

5 Federal Trade Commission [Internet]. Washington (DC): FTC. Press release, FTC files complaint against LabMD for failing to protect consumers' privacy. 2013 Aug 29 [cited 2014 Jan 6]. Available from: http://www.ftc.gov/opa/2013/08/labmd.shtm

6 For further technical discussion, see Luxton DD, Kayl RA, Mishkind MC. mHealth data security: the need for HIPAA-compliant standardization. Telemed J E Health. 2012;18(4): 284–8.

7 Mattsson UT. Everything enterprises need to know about end-to-end encryption [Internet]. Cos Cob (CT): Protegrity Corp.; [last updated 2009 Jun 11, cited 2014 Jan 6]. Abstract only available from: http://ssrn.com/abstract=1416856

8 National Institute of Standards and Technology, Information Security and Privacy Advisory Board. Minutes of meeting: October 10, 11, and 12, 2012 [Internet]. Gaithersburg (MD): NIST; 2013 Mar 8 [cited 2014 Jan 6]. Available from: http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-10/ispab_meeting-minutes_october-2012.pdf

9 45 CFR sec. 160.102, 164.104.

10 45 CFR sec. 164.312(a)(2)(iv) and (e)(2)(ii).

11 45 CFR sec. 160.103.

12 Department of Health and Human Services. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; other modifications to the HIPAA rules; final rule. Fed Regist. 2013;78(17):5565–702.

13 State laws regulating telehealth technologies are beyond the scope of this paper.

14 15 US Code secs. 41–58.

15 Solove DJ, Hartzog W. The FTC and the new common law of privacy. Columbia Law Review. Forthcoming 2014.

16 Yang YT, Silverman RD. Mobile health applications: the patchwork of legal and liability issues suggests strategies to improve oversight. Health Aff (Millwood). 2014;33 (2):222–27.

17 Food and Drug Administration. Content of premarket submissions for management of cybersecurity in medical devices: draft guidance for industry and Food and Drug Administration staff [Internet]. Silver Spring (MD): FDA; 2013 Jun 14 [cited 2014 Jan 6]. Available from: http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf

18 Food and Drug Administration. Radio frequency wireless technology in medical devices: guidance for industry and Food and Drug Administration staff [Internet]. Silver Spring (MD): FDA; 2013 Aug 14 [cited 2014 Jan 6]. Available from: http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077272.pdf

19 Food and Drug Administration. Mobile medical applications: guidance for industry and Food and Drug Administration staff [Internet]. Silver Spring (MD): FDA; 2013 Sep 25 [cited 2014 Jan 9]. Available from: http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf

20 Newton C. Fingerprint analysis: will the iPhone's newest sensor change the world again? The Verge [serial on the Internet]. 2013 Sep 10 [cited 2014 Jan 6]. Available from: http://www.theverge.com/2013/9/10/4716098/fingerprint-analysis-touch-id-sensor-iphone-5s

21 47 US Code sec. 551.

22 47 US Code sec. 222.

23 15 US Code sec. 1681 et seq.

24 15 US Code sec. 6801 et seq.

25 Department of Commerce, Internet Policy Task Force. Commercial data privacy and innovation in the Internet economy: a dynamic policy framework [Internet]. Washington (DC): DOC; 2010 Dec 16 [cited 2014 Jan 6]. Available from: http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf

26 Rubenstein I. Privacy and regulatory innovation: moving beyond voluntary codes. I/S, A Journal of Law and Policy for the Information Society. 2011;6:356.