Law and the Public's Health

One of the areas of greatest opportunity and challenge in health system transformation is addressing the needs of people with behavioral conditions. This installment of *Law and the Public's Health* examines the issues that arise at the intersection of health system reform and information exchange.

Sara Rosenbaum, JD
George Washington University, Milken Institute School of Public Health
Department of Health Policy, Washington, DC

REGULATION OF INFORMATION TECHNOLOGY IN BEHAVIORAL HEALTH

MELISSA M. GOLDSTEIN, JD

The potential for information technology (IT)-based therapeutic tools (e.g., mobile phone applications [apps] and portable sensors that connect to mobile devices) to enhance behavioral health at both the individual and population levels is great, although their use can present challenges. This installment of *Law and the Public's Health* focuses on one of the most complex challenges: how to regulate these tools to address issues of privacy and security. These questions arise as the use of IT in behavioral health care grows more widespread and sophisticated, and the number and types of entities involved in managing behavioral health information increase. How the legal environment should respond to this transformation in behavioral health treatment and management has emerged as a significant question in health information law.

BACKGROUND

Protecting the privacy and security of health information is a public health priority in the United States due to the harm that can occur when such information is disclosed inappropriately.¹ Discrimination, particularly by employers or insurers, as well as stigma and embarrassment, are all serious potential consequences related to the unauthorized disclosure of sensitive health information.² In the area of behavioral health interventions in particular, privacy concerns can be a significant barrier to accessing treatment.³

Recent technological advancements that enable health information to be shared electronically offer considerable promise for monitoring and responding to individuals' health behavior in real time, with the development of tools that may function as clinician extenders and allow tailoring to individual profiles

and behavior trajectories.⁴ The associated explosion in the availability and collection of health information, however, makes privacy and security concerns even more salient.⁵

For example, consider a hypothetical mobile phone app developed to provide cognitive behavioral therapy for depression. The app collects, shares, and analyzes video and audio recordings from a patient's phone, as well as photos, text messaging data, data from sensors (including global positioning system sensors and accelerometers), and data from connected tools such as sleep monitors.⁶ At the individual treatment level and in public health outreach settings, this app could provide valuable information to treatment teams, while also presenting opportunities for valuable aggregate data collection and sharing at the population health level. At each data collection point, however, and wherever data are stored or shared, entities such as device manufacturers, mobile network operators, app developers, data storage companies, or data analytics companies may also be accessing patient information, thereby presenting potential privacy and security issues.

HEALTH INFORMATION PRIVACY AND SECURITY LAW

HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is the primary federal law protecting the privacy and security of health information.⁷ HIPAA sets a privacy floor and preempts less stringent state laws. Any state laws that provide greater protection than HIPAA remain in force.⁸

The HIPAA Privacy and Security Rules⁹ address the circumstances under which a patient's individually identifiable health information (i.e., protected health information [PHI])¹⁰ can be disclosed, and the security measures that holders of health information should have in place. The regulations apply only to "covered entities," which are health plans, health care clearinghouses, and health care providers that

transmit health information electronically for specific purposes, including those related to health care claims and health plans.¹⁰

Generally, the Privacy Rule allows disclosure of PHI without patient authorization for the purposes of treatment, payment, or health care operations,¹¹ which include activities such as quality assessment or compliance audits. Additionally, a covered entity is permitted to disclose PHI in certain other circumstances, including disclosures for public health purposes or to comply with state or federal laws.¹²

Contractors and other organizations that conduct business on behalf of covered entities and that create, receive, maintain, or access PHI are considered “business associates” by HIPAA and must comply with all provisions of the Security Rule and most provisions of the Privacy Rule.⁹ Thus, entities that gain access to PHI, such as mobile app software vendors, may be considered business associates if they act on behalf of covered entities. As such, they may be responsible for complying with HIPAA.

Because HIPAA only applies to certain organizations, however, health IT products that are not offered by covered entities or their business associates, but that still collect or access health information (e.g., mobile health apps marketed directly to consumers), do not have to comply with the regulations, thereby exhibiting a regulatory gap in HIPAA’s protection of identifiable health data.¹³ In the absence of an overarching federal privacy law that provides baseline privacy protections to individuals, this gap is currently covered in part by agencies outside the U.S. Department of Health and Human Services.

42 C.F.R. Part 2

Some behavioral health information is also subject to 42 C.F.R. Part 2 (hereinafter, Part 2),^{14–16} federal regulations that address the disclosure of personal information related to substance use treatment. Part 2 applies to entities holding themselves out as substance use treatment providers who receive support from the federal government.¹⁷ The regulations protect any information from a Part 2 program that indicates directly or indirectly that a patient is a participant or has a current or past drug or alcohol problem.¹⁸

With limited exceptions (e.g., medical emergencies),¹⁹ a patient’s written consent is required to release information related to Part 2 treatment, and whenever such information is released, a statement prohibiting its redisclosure must accompany the information.²⁰ These requirements, which are more stringent than HIPAA’s, were adopted because of the sensitivity of substance use treatment information, the stigma asso-

ciated with it, and the strong public health interest in encouraging individuals with substance use issues to seek treatment.²¹

REGULATING MOBILE OR WEB-BASED TECHNOLOGIES

There is growing legal activity aimed at addressing the use of IT in consumer-facing products and services, including mobile health apps, health-related websites and Web-based services, and portable sensors that connect to mobile devices. Regulators include the Federal Trade Commission (FTC), the U.S. Food and Drug Administration (FDA), the National Telecommunications and Information Administration, the Federal Communications Commission, and some states. In general, these agencies’ efforts have emphasized industry self-regulation and transparency and have been guided by the Fair Information Practice Principles (FIPPS) (i.e., transparency and notice, individual consent, purpose specification, data minimization, use limitation, data integrity, security safeguards, and auditing).²² Key themes have emerged, such as enabling informed consumer choice through the provision of appropriate notice, expanding the types of personally identifying information that should be protected, and focusing on the collection of consumer data by third parties, including the communication of such activity to consumers.

The FTC

Under Section 5 of the Federal Trade Commission Act, the FTC has the authority to prevent “unfair or deceptive” acts related to commercial activity.²³ An act is considered unfair if it causes, or is likely to cause, substantial injury to a consumer that the consumer is not reasonably able to avoid, and that is not outweighed by benefits to the consumer.^{24,25} An act is considered deceptive if it involves a practice or representation that is likely to mislead a consumer acting reasonably and is also material to the consumer—that is, the practice or representation is likely to have kept the consumer from using the product had it not been misrepresented.²⁵

Generally, FTC enforcement actions addressing deceptive acts in the consumer IT arena have emphasized the importance of following stated privacy policies, including policies and practices described in privacy notices posted on an entity’s website, as well as user manuals.^{26,27} Violation of voluntary codes of conduct that an entity claims to follow could also lead to a deceptive practice enforcement action.²⁸ Regarding unfair acts, recent FTC enforcement activities have focused on the security measures that entities employ to protect consumer information, as well as the manner

in which entities allow third parties to access and use that information.²⁹

The FTC has issued privacy guidance for mobile apps and app developers that focuses on privacy disclosures and the process of marketing such apps. The guidance stresses the importance of “just in time” notices (which prompt consumers for permission at the time personal information is about to be collected) and obtaining affirmative consent when sensitive information (e.g., health information) is being collected or shared with third parties.³⁰

The FDA

Under the Food, Drug and Cosmetic Act, the FDA regulates devices that are intended for medical use, including software and hardware, for safety and efficacy.³¹ Whether or not a product is considered a medical device subject to FDA regulation depends primarily on the product's intended use, including how it is marketed. Generally, products intended for the diagnosis, cure, treatment, mitigation, or prevention of a medical condition are considered medical devices.³¹

Recent FDA guidance clarifies the types of health apps that the FDA will regulate, emphasizing that most would likely not be regulated. According to the guidance, the FDA will only regulate an app if it functions as a medical device (i.e., defined as “mobile medical apps”)—that is, it meets the definition of a device and it is either used as an accessory to a regulated medical device or it transforms a mobile platform into a regulated medical device, and it could pose a risk to patient safety if it did not function as intended.³² For example, the FDA might consider an app that analyzes electrocardiogram or other sensor data to detect heart problems to fall under its authority, but does not intend to regulate mobile apps that help patients with psychiatric conditions through delivery of messages or tips to improve coping skills; apps that provide education, reminders, or motivation to patients recovering from addiction; or general wellness apps.^{32,33}

RECENT DEVELOPMENTS

As technology rapidly advances, regulators continue to work to keep pace with technology. Of particular note is the Substance Abuse and Mental Health Administration's activity regarding potential updates to Part 2. In June 2014, the agency held a listening session to seek public input on potential changes to the regulations, including measures important to population health, such as when data can be released for research, how the regulations work with prescription drug monitoring programs, and clarification that population health

management and care coordination are appropriate third-party services for Part 2 programs.³⁴ Although the agency's timing is not clear, any proposed changes will be released to the public with an opportunity for comment before finalization.

In addition, a diverse federal workgroup that includes the FDA, the Federal Communications Commission, and the Office of the National Coordinator for Health Information Technology within the U.S. Department of Health and Human Services is currently exploring the creation of a non-duplicative risk-based regulatory framework that protects patient safety in health IT, including mobile medical apps.³⁵ With respect to privacy and security issues, the agencies have emphasized the importance of examining and considering network security risks and compliance with security standards as part of any resulting regulatory framework.³⁶

Finally, the Obama Administration recently released the discussion draft of the Consumer Privacy Bill of Rights Act of 2015,³⁷ which expands upon principles (based upon the FIPPS) outlined by the Administration in 2012.³⁸ The proposal creates a comprehensive framework for national consumer privacy and is part of the Administration's effort to combat cyber threats while safeguarding consumer privacy and civil liberties.³⁹

IMPLICATIONS FOR PUBLIC HEALTH POLICY AND PRACTICE

Although it has been estimated that the mobile health app market will increase annually by 25% for the foreseeable future,⁴⁰ some lawmakers have pressed for affirmative deregulation in the area⁴¹ based upon the assumption, repeatedly echoed by industry, that broad regulation could increase the cost and time associated with technological development.^{42,43} Others argue, however, that regulation is a required facilitator for industry change—instead of hindering growth, providing a regulatory structure encourages interoperability and can support the evolution of existing markets instead of allowing disruptive new markets to displace older technologies.⁴⁴

As regulators navigate the proper balance between innovation in the collection of health information and fair data practice controls, policy makers ultimately need to address the broader social consequences of pervasive health information collection, aggregation, and use.⁴⁵ As we move forward, embracing the core principles of appropriately sharing health information, providing adequate notice and choice to patients, and ensuring proper security safeguards will help enable the use of IT within behavioral health care in a way

that both protects the privacy and security of sensitive health information and inspires patient trust.¹³

Melissa Goldstein is an Associate Professor at the George Washington University Milken Institute School of Public Health in Washington, DC.

Address correspondence to: Melissa M. Goldstein, JD, George Washington University, Milken Institute School of Public Health, 950 New Hampshire Ave. NW, 2nd FL, Washington, DC; tel. 202-994-4235; e-mail <mgoldste@gwu.edu>.

©2015 Association of Schools and Programs of Public Health

REFERENCES

- Beckerman JZ, Pritts J, Goplerud E, Leifer JC, Borzi PA, Rosenbaum S, et al. A delicate balance: behavioral health, patient privacy, and the need to know. Oakland (CA): California HealthCare Foundation; 2008. Also available from: URL: <http://www.chcf.org/publications/2008/03/a-delicate-balance-behavioral-health-patient-privacy-and-the-need-to-know> [cited 2015 Jan 20].
- Gostin LO, Hodge JG Jr, Valdiserri RO. Informational privacy and the public's health: the Model State Public Health Privacy Act. *Am J Public Health* 2001;91:1388-92.
- Rapp RC, Xu J, Carr CA, Lane T, Wang J, Carlson R. Treatment barriers identified by substance abusers assessed at a centralized intake unit. *J Subst Abuse Treat* 2006;30:227-35.
- Marsch LA, Lord SE, Dallery J, editors. Behavioral healthcare and technology: using science-based innovations to transform practice. New York: Oxford University Press; 2015.
- Goldstein MM, Rein AL. Data segmentation in electronic health information exchange: policy considerations and analysis. Washington: Department of Health and Human Services (US), Office of the National Coordinator for Health Information Technology; 2010. Also available from: URL: <http://www.healthit.gov/sites/default/files/privacy-security/gwu-data-segmentation-final.pdf> [cited 2015 Jan 20].
- Thomson Reuters Foundation. Patient privacy in a mobile world: a framework to address privacy law issues in mobile health. London: Thomson Reuters Foundation; 2013. Also available from: URL: <http://www.trust.org/contentAsset/raw-data/03172beb-0f11-438e-94be-e02978de3036/file> [cited 2015 Jan 20].
- Pub. L. No. 104-191, 110 Stat. 1936 (1996).
- 45 C.F.R. §160.203.
- 45 C.F.R. §§160, 164.
- 45 C.F.R. §164.103.
- 45 C.F.R. §164.506.
- 45 C.F.R. §164.512.
- Goldstein MM, Pewen WF. The HIPAA Omnibus Rule: implications for public health policy and practice. *Public Health Rep* 2013;128:554-8.
- Pub. L. No. 91-616, 84 Stat. 1848 (1970).
- Pub. L. No. 92-255, 86 Stat. 65 (1972).
- 42 U.S.C. §290dd-2.
- 42 C.F.R. §2.11.
- 42 C.F.R. §2.12.
- 42 C.F.R. §2.51.
- 42 C.F.R. §2.3.
- 42 C.F.R. §2.3(b)(2).
- Advisory Committee on Automated Personal Data Systems. Records, computers, and the rights of citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems. Washington: Department of Health, Education and Welfare (US); 1973. DHEW Pub. No. (OS) 73-94.
- 15 U.S.C. §45(a)(1),(2).
- 15 U.S.C. §45(n).
- 15 U.S.C. §45(a)(4)(A).
- FTC v. Toysmart.com, LLC*, 2000 WL 34016434 (D. Mass. July 21, 2000) (unreported).
- Federal Trade Commission (US). In the matter of HTC America Inc. FTC file no. 122 3049 (2013) (complaint) [cited 2015 Mar 8]. Available from: URL: <http://ftc.gov/os/caselist/1223049/130702htccmpt.pdf>
- Federal Trade Commission (US). In the matter of Google, Inc., a corporation. FTC file no. 102 3136 (2011) (complaint) [cited 2015 Jan 20]. Available from: URL: <http://www.ftc.gov/os/caselist/1023136/index.shtm>
- Federal Trade Commission (US). In the matter of Ceridian Corporation, a corporation. FTC file no. 102 3160 (2011) (complaint) [cited 2015 Jan 20]. Available from: URL: <http://www.ftc.gov/os/caselist/1023160/index.shtm>
- Federal Trade Commission (US). Mobile privacy disclosures: building trust through transparency: a Federal Trade Commission staff report. February 2013 [cited 2015 Jan 20]. Available from: URL: www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf
- 21 U.S.C. §321(h).
- Department of Health and Human Services (US), Food and Drug Administration (US). Mobile medical applications: guidance for industry and Food and Drug Administration staff. 2015 Feb 9 [cited 2015 Feb 17]. Available from: URL: <http://www.fda.gov/medicaldevices/productsandmedicalprocedures/connectedhealth/mobilemedicalapplications/default.htm>
- Department of Health and Human Services (US), Food and Drug Administration (US), Center for Devices and Radiological Health. General wellness: policy for low risk devices: draft guidance for industry and Food and Drug Administration staff. 2015 [cited 2015 Jan 20]. Available from: URL: <http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM429674.pdf>
- Substance Abuse and Mental Health Services Administration (US). Confidentiality of alcohol and drug abuse patient records: a proposed rule by the Substance Abuse and Mental Health Services Administration (notice of public listening session). 2014 May 12 [cited 2015 Jan 20]. Available from: URL: <https://www.federalregister.gov/articles/2014/05/12/2014-10913/confidentiality-of-alcohol-and-drug-abuse-patient-records>
- Pub. L. No. 112-144, 126 Stat. 993, §618 (2012).
- Department of Health and Human Services (US), Food and Drug Administration (US). FDASIA health IT report: proposed strategy and recommendations for a risk-based framework. April 2014 [cited 2015 Jan 20]. Available from: URL: <http://www.fda.gov/aboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHReports/ucm390588.htm>
- The White House (US). Administration discussion draft: Consumer Privacy Bill of Rights Act of 2015. 2015 Feb 27 [cited 2015 Mar 5]. Available from: URL: <http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf>
- The White House (US). Consumer data privacy in a networked world: a framework for protecting privacy and promoting innovation in the global digital economy. February 2012 [cited 2015 Jan 20]. Available from: URL: www.whitehouse.gov/sites/default/files/privacy-final.pdf
- The White House (US). Fact sheet: safeguarding American consumers & families. 2015 Jan 12 [cited 2015 Jan 20]. Available from: URL: <http://www.whitehouse.gov/the-press-office/2015/01/12/fact-sheet-safeguarding-american-consumers-families>
- Orr E. 2011 in review: MDUFA, 510(k) debate made list of top news. *Devices & Diagnostics Letter* 2. 2012 Jan 2 [cited 2015 Mar 8]. Available from: URL: <http://www.fdanews.com/articles/142851-2011-in-review-mdufa-510-k-debate-made-list-of-top-news?v=preview>
- Cortez C. The mobile health revolution? 47 U.C. Davis L Rev 2014;47:1173-230.
- McGowan JJ, Cusack CM, Bloomrosen M. The future of health IT innovation and informatics: a report from AMIA's 2010 policy meeting. *J Am Med Inform Assoc* 2012;19:460-7.
- Cooper D. Notes: understanding the impact of the FDA guidance for mobile medical applications: is there an app for that? 32 *Quinnipiac L Rev* 2013;95:112-3.
- Wanderer J, Mishra P, Ehrenfeld J. Innovation & market consolidation among electronic health record vendors: an acute need for regulation. *J Medical Systems* 2014;38:8.
- Pasquale F, Goldstein MM. Regulatory landscape II: looking forward. Presentation at Exploring Legal Challenges to Fulfilling the Potential of mHealth in a Safe and Responsible Environment, a workshop sponsored by the American Association for the Advancement of Science; 2014 Jun 16-17; Washington.