Telemedicine and mobile health innovations amid increasing regulatory oversight

By Sharon Klein, Esq., and Jee-Young Kim, Esq.
Pepper Hamilton LLP

The growing mobile health market is rapidly transforming health care delivery. More than 80 percent of physicians use mobile technology to provide patient care, and more than 25 percent of commercially insured patients use mobile applications to manage their health.[1]

Technological advancements, the expansion of access to health care under the Patient Protection and Affordable Care Act, Pub. L. No. 111-148, the emphasis on cost-effective quality care and the proliferation of mobile medical applications have pushed telemedicine to the new frontier of health care delivery.

Over the past 50 years, the scope of telemedicine practices has expanded to meet demands for immediate care in both remote and metropolitan regions. Mobile health, a form of telemedicine using wireless devices and cell phone technologies, has also evolved. By the end of this year, experts expect 2 billion smartphones, tablets and other portable devices globally, each of which can potentially provide individuals access to health care information from anywhere at any time.[2]

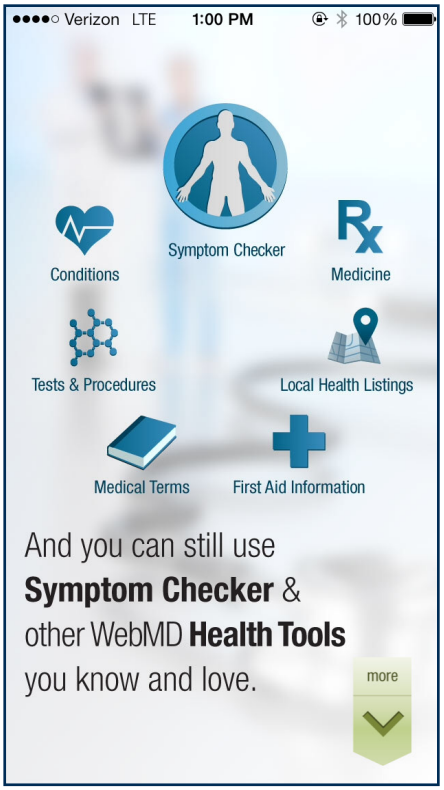
In light of the seemingly limitless opportunities in telemedicine, health care providers, consumers and entrepreneurs must navigate the many risks that come with reliance on these new technologies and comply with an increasing number of regulations.

UNDERSTANDING TELEMEDICINE AND MOBILE HEALTH

Telemedicine involves direct patient care and is a subcategory of telehealth, a broader concept that includes telecommunications technologies, or mobile medical applications, to remotely support health care, health-related education, public health and health administration.[3] Generally, telemedicine involves:

- Geographic separation between two or more participants or entities engaged in health care.
- The use of telecommunications technology to gather, store and disseminate health-related information.
- The use of interactive technologies to assess, diagnose and treat medical conditions.

Mobile health is a medium through which telemedicine is practiced. It allows for increased provider and patient mobility, as well as greater delivery of clinical care via consumer-grade hardware, such as smartphones and tablets.[4]



The WebMD app is shown here. WESTLAW JOURNAL/Kim Sachs

> Mobile health allows for greater provider and patient mobility and the delivery of clinical care via consumer-grade hardware, such as smartphones and tablets.

Sharon R. Klein (L) is the partner-in-charge of **Pepper Hamilton LLP**'s office in Orange County, Calif., where she serves as the national chair of the privacy, security and data protection practice. She can be reached at kleins@pepperlaw.com. **Jee-Young Kim** (R) is an associate in the firm's health care services practice in the Los Angeles office. She can be reached at kimjy@pepperlaw.com.

RECENT TELEMEDICINE AND MOBILE HEALTH TRENDS

The resurgence of telemedicine began in 2011, when the U.S. Centers for Medicare & Medicaid Services issued a much-awaited final rule permitting a more flexible process for credentialing and privileging practitioners who provide these services. The trend escalated in 2013, when federal and state legislation and major insurers expanded the types of reimbursable telemedicine services. In 2014, the trend continues with the Federation of State Medical Boards' adoption of a model policy intended to provide guidance to state medical boards

for regulating the use of telemedicine technologies.[5]

Increasingly, there are more arrangements for distant-site specialists to provide tele-ICU (intensive care unit), tele-stroke and other telemedicine services; partnerships between insurers and integrated health care delivery systems to provide patients in rural communities access to specialists through telemedicine programs; and development of mobile technology for patient monitoring, patient engagement and virtual clinical encounters.

Within the mobile health industry, pharmacy management continues to be the most common use of mobile technologies. Growth will most likely continue as data analytics vendors launch hosting platforms that make it easier for mobile application developers to comply with federal privacy and security requirements in the health care arena.

NAVIGATING LEGAL ISSUES IN TELEMEDICINE AND MOBILE HEALTH

As more health care entities use telemedicine, more consumers rely on these and mobile health services, and more entrepreneurs develop telemedicine technologies, oversight and scrutiny by state medical boards and federal and state regulatory agencies also continue to increase.

Providers, consumers and entrepreneurs must be mindful of the following legal issues to ensure their telemedicine and mobile health services are compliant with federal and state requirements, and appropriately protect patient safety and privacy.

PROVIDER CONSIDERATIONS

Reimbursement

Reimbursement continues to be a significant barrier to telemedicine. Medicare reimbursement for telemedicine services is limited. Generally, it requires face-to-face contact between a patient and provider, with exceptions for certain telemedicine services provided at eligible facilities located in rural, non-metropolitan areas with health care professional shortages.

Medicaid reimbursement varies from state to state, and only about 20 states have enacted statutes that recognize or require commercial insurers to reimburse for certain telemedicine services.

Providers should be aware of the reimbursement requirements and restrictions that may affect their billing practices, know which telemedicine services will be reimbursed and only submit compliant claims to avoid liability for fraud and abuse or false claims.

Fraud and abuse

Telemedicine services often involve business arrangements between unrelated health care entities and may include the lease of equipment or the use of a product owned in part by physicians. Such business arrangements must be structured in a manner that does not implicate federal fraud and abuse laws, including the Anti-Kickback Statute and the Stark Law.

> Increasingly, there are more arrangements for distant-site specialists to provide emergency, stroke and other telemedicine services.

Under the Anti-Kickback Statute, it is a crime to knowingly offer, pay, solicit or receive any remuneration to induce referrals of items or services reimbursable by a federal health care program.[6] Arrangements meeting certain requirements that are set forth in regulatory safe harbors do not implicate the statute.

The Stark Law prohibits physicians from referring Medicare patients for designated health services to an entity with which the physician has a financial relationship.[7] It includes exceptions that apply to ownership interests and compensation arrangements involving physicians.

Advisory opinions issued by the U.S. Department of Health and Human Services' Office of Inspector General addressing telemedicine-related fraud issues provide additional guidance for providers and entrepreneurs when structuring telemedicine arrangements.[8]

Medical staff bylaws

Health care organizations that provide telemedicine services must review and revise their medical staff bylaws and credentialing and privileging policies to make sure they cover telemedicine practitioners and practices. These documents must include criteria for granting privileges to distant-site practitioners and a procedure for applying the criteria to those practitioners.[9] They should also address what category of the medical staff distant-site telemedicine practitioners will join, the level of involvement they may have in medical staff committees and the procedural rights they will enjoy.

Credentialing and privileging

Regardless of telemedicine advancements, health care organizations remain liable for the care provided to their patients. Under CMS' final rule, effective July 5, 2011, health care organizations may rely on the credentialing and privileging decisions of distant-site hospitals or information provided by other telemedicine entities when determining privileges for practitioners who provide telemedicine services as long as certain conditions are met, including a compliant written agreement.[10]

To mitigate possible negligent credentialing claims and associated risks, when entering into written agreements with distant sites, health care organizations must know who will be providing care to patients, confirm that any written agreement they sign reflects current legal requirements and establish specific responsibilities of distant-site hospitals and telemedicine entities. They must also ensure that written agreements include adequate representations, warranties and indemnifications regarding the quality of services provided by the distant site and any entity with which it subcontracts.

Distant sites, in turn, must have processes to assess the quality of their practitioners. While distant-site, Medicare-participating hospitals are highly regulated, distant-site telemedicine entities are not. Therefore, relationships with such entities require greater scrutiny to assure the quality of the telemedicine services being provided and the qualifications of the practitioners providing them.

Peer review

The expansion and increased reliance on telemedicine means that health care organizations and telemedicine entities must develop policies and procedures for monitoring telemedicine practitioners and sharing internal review information. While

information needed to make accurate credentialing and privileging decisions should be regularly shared, it must be done in a manner that maintains and protects the privacy of peer review and patient information.

At a minimum, this shared information must include adverse events that result from a practitioner's telemedicine services and complaints a health care organization

> Reimbursement continues to be a significant barrier to telemedicine.

receives about a practitioner.[11] Health care organizations should determine what additional information, if any, to collect, how to use and act on this information and what information to share so that all peer-review privileges under state law are preserved.

Compliance with state requirements

Most states continue to require physicians engaging in telemedicine to be licensed in the state where the patient is located, with limited exceptions for consultations. For telemedicine and mobile health services, health care organizations and providers need expert legal guidance to navigate individual state requirements, including licensure, consent and patient notice and practice of medicine issues, and the possible exceptions to such requirements.

CONSUMER AND PATIENT CONSIDERATION

Patient privacy

Entrepreneurs are continuing to develop mobile medical applications for virtual physician-patient and clinical interactions across the continuum of care. These include payment portals and applications dedicated to medication management, fitness and consumer health.

Prior to relying on any telemedicine technology to collect and transfer patients' protected health information, health care entities should ensure that they have secure communication channels; implement entity- and technology-specific business associate and other confidentiality and privacy agreements; educate administrators and users regarding the appropriate use of telemedicine technologies; and understand how and what patient information is being collected, transmitted, used and stored.

When information is shared between unrelated entities, all disclosures must comply with federal and state privacy and security laws, including the Health Insurance Portability and Accountability Act, or HIPAA, Pub. L. 104-191, and the Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, and guidance by the Federal Trade Commission.

As a result of modifications to federal privacy and security laws in 2013, all subcontractors having access to protected health information (no matter how far down the chain) must now comply with the full spectrum of requirements applicable to business associates.[12]

With the development of mobile applications, the Federal Trade Commission and U.S. Department of Health and Human Services are recognizing that health data is moving beyond the traditional medical-provider context and falling outside the scope of federal and state privacy laws as more consumers are managing and controlling their own health data.

HHS has announced that its Office of Inspector General intends to review the security of portable devices used in hospitals that access protected health information as part of its HIPAA compliance audits.[13] Emphasis is being placed on transparency and clear notice to consumers about how their health data is being collected, stored, and shared when provided through mobile applications.[14]

TECHNOLOGY AND VENDOR CONSIDERATIONS

Regulatory overlap

Developers and manufacturers of mobile health applications and devices that support telemedicine services must comply with multiple, and often conflicting, privacy and security regulations promulgated by various federal agencies:

- The Food and Drug Administration establishes regulations regarding the hardware and software, including the safety and effectiveness, of telemedicine devices and mobile medical applications.
- The Federal Communications Commission establishes regulations regarding interstate and international communications by airwaves, including wireless technology issues and problems with connectivity, as well as technical regulations for transmitters and other equipment.
- The Federal Trade Commission establishes regulations regarding disclosures about the collection and use of consumer data to avoid false, misleading and deceptive trade practices and provides a privacy-by-design framework for protecting mobile privacy. The FTC is currently examining health care competition, including regulatory barriers that may prevent telemedicine across state lines.
- The Office of National Coordinator for Health Information Technology, or ONC, establishes regulations to adopt standards and certification criteria for health information technology.

Inter-agency collaboration

Given the potentials for overlap, in 2012, through the FDA Safety and Innovation Act, Congress required the Food and

> Providers should be aware of the reimbursement requirements and restrictions that may affect their billing practices.

Drug Administration to consult with the FCC and ONC to develop a report with recommendations for a risk-based regulatory framework pertaining to health IT that avoids regulatory duplication.

On April 3, 2014, HHS released the draft report prepared by the FDA, FCC and ONC,[15] which identified three categories of health IT, based on function and level of risk to patient safety, rather than the platform on which it operates:

- Administrative health IT functions, such as billing and scheduling.
- Health management health IT functions, such as health information and data exchange, electronic access to clinical results, and medication management.
- Medical device health IT functions, such as computer aided detection software

FDA's guidance to developers and manufacturers on mobile medical apps	
Mobile applications that are considered medical devices and subject to FDA regulations	• Applications that are intended to be used as an accessory to a medical device to control the device or display patient-specific data. • Applications that transform the mobile platform into a medical device with attachments or sensors. • Applications that perform patient-specific analysis and assist with diagnosis or treatment recommendations.
Mobile applications that may be considered medical devices, but which the FDA does not currently intend to regulate	• Applications that supplement clinical care by helping patients manage their health. • Applications that help patients document or communicate their medical information to providers. • Applications that perform simple calculations used in clinical practice.
Mobile applications that could be used in a health care environment, but are not considered medical devices	• Electronic copies of reference materials. • Educational tools for medical training. • Applications used for general patient education. • Applications that automate general office operations in a health care setting.

and robotic surgical planning and control.

The agencies concluded that the administrative and health management functions posed little risk to patient safety and required either no or limited additional oversight. However, because of their recognized risks, medical device health IT functions would remain under FDA oversight.

This proposed functional categorization emphasizes that the safety of health IT relies not only on how it is designed and developed, but also on how it is customized, implemented, integrated and used by clinicians, patients and vendors.

> Most states continue to require physicians engaging in telemedicine to be licensed in the state where the patient is located, with limited exceptions for consultations.

FDA guidance

Recently, the FDA has been active in regulating mobile health, extending its jurisdiction into health care information technology and redefining medical devices to include software applications, including mobile medical applications. In 2013 it issued guidance for developers and manufacturers on what mobile medical applications qualify as a medical device and further guidance on cybersecurity concerns in this market.

On Sept. 25, 2013, the FDA issued a final guidance on mobile medical applications to provide clarity for developers and manufacturers regarding regulatory oversight.[16] According to the agency, whether a mobile application constitutes a medical device that is subject to FDA regulation depends on its intended use.[17] Specifically, the FDA guidance separates mobile applications into three categories (see box).

The regulatory overlap surrounding mobile medical applications is complex and likely to change as federal agencies continue to interact. Even if a mobile application is not currently subject to FDA regulation, the application may be subject to other federal and state agency regulations.

On June 14, 2013, the FDA issued draft guidance on medical device cybersecurity that supplements existing policies[18] and addresses issues that manufacturers should consider when designing medical devices to effectively mitigate these risks.[19] Such risks include the intentional or unintentional compromise of a device or its stored data. According to the agency, medical devices capable of connecting to another medical device, the Internet or other network, or portable media are more vulnerable to cybersecurity threats than those that are not connected.

The FDA recommends manufacturers develop security controls to maintain the confidentiality, integrity, and availability of information stored in medical devices. Additionally, cybersecurity issues and risks should be addressed and analyzed in the design phase, both for efficiency in the FDA approval process and greater effectiveness in managing a device's security.

CONCLUSION

Increased use of mobile medical technology comes with heightened regulations to mitigate the privacy and security risks of the interconnected health care environment. The absence of comprehensive national privacy and security legislation has driven regulatory agencies to step in.

To navigate the multifaceted legal complexities of telemedicine and mobile health, health care companies should appoint an interdisciplinary committee to monitor regulatory guidance, assess common compliance principles across regulatory agencies, document compliance with privacy and security criteria, perform regular risk analysis for privacy and security issues and develop incident response programs. WJ

NOTES

[1] Press Release, Healthcare Info. & Mgmt. Sys. Soc'y Analytics, HIMSS Analytics 2013 Mobile Technology Survey Examines mHealth Landscape (Feb. 26, 2014), http://bit.ly/1uBlbFa; Matt Mattox, *10 Key Statistics about mHealth* (Jan. 15, 2013), http://bit.ly/1lwaaFr.

[2] IMS Inst. for Healthcare Informatics, *Patient Apps for Improved Healthcare: From Novelty to Mainstream* (October 2013), *available at* http://bit.ly/1lwajsG.

[3] The Centers for Medicare and Medicaid Services defines telemedicine as "the provision of clinical services to patients by practitioners from a distance via electronic communications." 76 Fed. Reg. 25,553 (May 5, 2011).

[4] Am. Telemedicine Ass'n, Telemedicine Frequently Asked Questions, What is mHealth?, http://bit.ly/1pdl6Gj.

[5] The Federation of State Medical Boards defines telemedicine technologies as "technologies and devices enabling secure electronic communications and information exchange between a licensee in one location and a patient in another location with or without an intervening health care provider." Fed'n of State Med. Bds., State Medical Boards' Appropriate Regulation of Telemedicine (SMART) Workgroup, Model Policy for the Appropriate Use of Telemedicine Technologies in the Practice of Medicine (Apr. 26, 2014), *available at* http://bit.ly/1ibJadE.

[6] 42 U.S.C. § 1320a-7b.

[7] 42 U.S.C. § 1395nn.

[8] *See generally* U.S. Dep't of Health & Human Servs., Office of Inspector Gen., Advisory Opinions, *available at* http://1.usa.gov/1nNDB4B.

[9] 42 C.F.R. §§ 482.12(a)(8), (a)(9); *see also* CMS State Operations Manual, Appendix A-Survey Protocol, Regulations and Interpretive Guidelines for Hospitals, Interpretive Guidelines for §§ 482.12(a)(8) & (a)(9).

[10] 42 C.F.R §§ 482.12(a)(8), (a)(9).

[11] 42 C.F.R. §§ 482.22(a)(3)(iv), (a)(4)(iv).

[12] 45 C.F.R. §§ 160.103; *see also* Rebekah Monson, Sharon Klein & Henry Fader, *The Omnibus Final HIPAA Rule Is Here,* Pepper Hamilton LLP Health Care Law Alert (Jan. 24, 2013), *available at* http://bit.ly/1nimm9Q.

[13] U.S. Dep't of Health & Human Servs., Office of Inspector Gen., *Work Plan for Fiscal Year 2014,* at 26, *available at* http://1.usa.gov/1kL18OM.

[14] Allison Grande, *Health Apps Need More Privacy Safeguards, FTC Panel Says,* Law360 (May 7, 2014), *available at* http://bit.ly/UJ01KL; *see also* Sharon R. Klein & Jeffrey L. Vagle, *FTC Recommends Framework for Mobile Privacy,* Pepper Hamilton LLP Client Alert (Feb. 25, 2013), *available at* http://bit.ly/1l0TPYi.

[15] Press Release, U.S. Dep't of Health & Human Servs., Proposed health IT strategy aims to promote innovation, protect patients, and avoid regulatory duplication (Apr. 3, 2014); *see also* U.S. Food & Drug Admin., Fed. Commc'ns Comm'n & Office of Nat'l Coordinator for Health Info. Tech., *FDASIA Health IT Report: Proposed Strategy and Recommendations for a Risk-Based Framework* (April 2014), *available at* http://1.usa.gov/1oBNDZZ.

[16] U.S. Food & Drug Admin., *Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff* (Sept. 25, 2013), *available at* http://1.usa.gov/1lBzw3p. The FDA guidance defines a "mobile application" as a software application that can be run on a mobile platform, or a Web-based software application that is tailored to a mobile platform but is executed on a server, and a "mobile medical application" as a mobile application that meets the statutory definition of a "device" and either is intended to be used as an accessory to a regulated medical device, or to transform a mobile platform into a medical device.

[17] Sharon R. Klein & Dayna C. Nicholson, *When Is an iPad More Than an iPad? When It Is an FDA Regulated Medical Device,* Pepper Hamilton LLP Client Alert (Mar. 7, 2014), *available at* http://bit.ly/1uBneZU.

[18] *See* U.S. Food & Drug Admin., *Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices* (May 11, 2005), *available at* http://1.usa.gov/1lBzGaK; *U.S. Food & Drug Admin., Guidance to Industry: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (COTS) Software* (Jan. 14, 2005), *available at* http://1.usa.gov/1pFTVYd.

[19] *See* U.S. Food & Drug Admin., *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices* (June 14, 2013), *available at* http://1.usa.gov/T7ls6K; *see also* Sharon R. Klein & Odia Kagan, *Unhack My Heart: FDA Issues Guidance to Mitigate Cybersecurity Threats in Medical Devices*, Pepper Hamilton LLP Client Alert (June 24, 2013), *available at* http://bit.ly/1iarYpf.