DuaneMorris®

mHealth Newsletter

Providing a cross-industry look at the latest trends in mobile healthcare and their impact on your business.

IN THIS ISSUE

VISIT US ONLINE

www.duanemorris.com/site/mhealth.html

http://dnmrs.co/g417

In the second issue of Duane Morris' *mHealth Newsletter*, we are pleased to share with you our further impressions on mobile health, a rapidly evolving sector of the healthcare industry that exemplifies innovation and is destined to reduce the costs and improve the quality of healthcare through mobile technology. Our attorneys continue to keep pace with the key factors that drive further convergence of healthcare and technology.

Nothing comes easy, especially with a field that is new, enterprising and breaks from traditional models. The mHealth marketplace is teeming with solutions that promote patient engagement by harnessing technology to enhance the patient's ability to communicate with his or her provider. This issue of *mHealth* will explore the particular privacy, security and other legal risks and requirements that arise any time a patient becomes more directly involved in his or her care, especially in the mHealth arena. In addition, mHealth investors and entrepreneurs may struggle to understand what business opportunities are present in the U.S. healthcare system since the passage of the Patient Protection and Affordable Care Act, and we will discuss how many of the Act's provisions offer mHealth entrepreneurs and investors new business opportunities and sources of revenue. We will also examine the natural fit that exists between home health and mobile health, given that, except for home visits and doctor's visits, patients and providers are not in the same place. The vital role of the Federal Communications Commission with mHealth issues will be highlighted, and if recent developments are any indication, that role will likely grow. Finally, we will report on AliveCor's strategy of pursuing a veterinary medicine use for the mobile electrocardiogram system it developed, even pending FDA clearance of its human model—which is a creative development in the mHealth arena that mobile medical application developers may want to emulate.

Lisa Clark, Editor
P: 215.979.1833
lwclark@duanemorris.com

BY-LINED ARTICLE

The P's & Q's of mHealth and Patient Engagement; Privacy and Security Issues

By Lisa Clark

November 14, 2012
mHealth Newsletter

"*Patient engagement* is the holy grail of healthcare,"[1] according to one hospital executive. Indeed, there is real money in the development of products and systems that support the patient's involvement in his or her healthcare. The mHealth marketplace is teeming with solutions that promote patient engagement by harnessing technology to enhance the patient's ability to communicate with his or her provider. For example, an mHealth product may permit a patient to email, text or video chat with the provider, or receive lab and other results. It is unlikely to come as a surprise that particular privacy, security and other legal risks and requirements arise any time a patient becomes more directly involved in his or her care, especially in the mHealth arena. This article offers a sampling of some of these requirements. Please keep in mind that the specific use of the mHealth solution will determine what laws apply.

Electronic Health Records

Many mHealth products are intended to interact with electronic health records (EHRs). The Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) allocated roughly $20 billion to provide financial incentives to hospitals, physicians and others for the adoption of EHRs. To be eligible for incentive payments, an eligible entity must demonstrate that it is a "meaningful user" of EHR technology by satisfying certain objectives and standards. The intent of the EHR initiative under HITECH is that by incentivizing hospitals, physicians and others key healthcare entities to adopt meaningful use EHR technology, ultimately all providers and payers (*e.g.*, skilled nursing homes, commercial payers, etc.) would have to use the same technology.

On September 4, 2012, the U.S. Department of Health and Human Services (HHS) issued the Stage 2 Meaningful Use Regulations that include several core objectives to promote patient engagement through EHR technology. Specifically, under the Stage 2 Meaningful Use Regulations, a provider must demonstrate that its EHR is able to perform certain tasks with a defined percentage of its patients: 1) to send messages to and from the patient; 2) the permit the patient to view online, download and transmit his or her health information within certain time frames; and 3) to identify patient-specific education resources and provide those resources to the patient. Ultimately, a provider's EHR technology will have to be able to meet these core objectives for all of its patients. HHS will add further meaningful use requirements over the next few years.

Those mHealth solutions that are designed to operate with EHRs have to comply with the certification standards, specifications and criteria specifically established for EHRs by regulation. With respect to secure messaging, this means that the product must encrypt and hash health information according to certain National Institute of Standards and Technology (NIST) standards. Therefore, any mHealth solution that falls under the EHR regulations must ensure compliance.

HIPAA

HIPAA protects the use and disclosure of protected health information (PHI) by hospitals, payers and billing companies, as well as their third-party business associates. PHI includes any data that clearly identifies (names, addresses, Social Security numbers, etc.) or could be used to identify an individual (images or medical record numbers). Virtually any time one of these entities uses or shares PHI, including to permit patient engagement with a provider through a mobile solution provided by a third party, the HIPAA standards apply.

Potential HIPAA privacy and security issues arise when a provider engages with a patient by allowing him or her to access medical records or through secure messaging. The biggest risk is that a person who is not the patient gains access to the patient's medical records, or messages with the provider. HHS will have to spell out how a provider can satisfy these privacy concerns while meeting the Stage 2 Meaningful Use Regulations' patient engagement objectives.

The HIPAA security standards impose specific requirements on the use and disclosure of electronic protected health information (ePHI) that would include any information transmitted wirelessly through an mHealth product. Although the HIPAA security standards do not specifically require encryption, it is implicitly recommended. Further, data that are breached but that are encrypted according to NIST standards adopted by HHS are not subject to the cumbersome HIPAA data-breach reporting rules. Strong encryption protection would ensure that hackers do not access the ePHI through a patient engagement feature of an EHR system. However, the system would still need to address the issue of how to verify the patient's identity in the case to guard against the practical concern that even if an individual has the tools necessary to access the ePHI or communicate with the provider, that individual may not be the patient (*e.g.*, a person accessing the records of his or her spouse without permission).

It may also be worthwhile to keep in mind other key HIPAA standards, such as requirements for privacy statements, passwords, audit controls and many others. Any entity that is subject to HIPAA, including an mHealth developer that is a business associate to a healthcare provider or plan, should consider how to ensure that the PHI does not get into the wrong hands if a device is stolen. In 2006, HHS issued Security Rule Guidance on Remote Access to PHI that imposes a high standard of compliance on remote users. Until the guidance is replaced or amplified, all mHealth products should be reviewed against the guidance, as well as HIPAA in general, to potentially minimize any HIPAA risks.

Non-Healthcare Specific Privacy Issues for Mobile Apps and Devices

Any mHealth solution, including one in which the patient and the provider interact, is governed not just by the laws and guidance applicable to the healthcare industry but also to the mobile industry. Under its authority to monitor unfair and deceptive practices, the Federal Trade Commission (FTC) is very active in enforcing mobile privacy policies on a number of fronts. Pursuant to HITECH, the FTC oversees enforcement with respect to the protection of personal data held in personal health records, those electronic and other records maintained by the patient (that the patient may choose to share with the provider). In September 2012, the FTC issued a guide to help mobile app developers observe truth-in-advertising and basic privacy principles called "Marketing Your Mobile App: Get It Right from the Start." Recently, the Government Accountability Office has recommended to Congress that the FTC issue guidance on the appropriate actions for mobile companies related to protecting mobile location privacy.

Other oversight bodies have weighed in on mobile privacy for consumers (including patients), notably the Attorney General of California. The California Online Privacy Protection Act requires that mobile app providers conspicuously post and adhere to privacy policies that inform the user how his or her data are being used. In late October 2012, California Attorney General Kamala Harris issued a statement that she would begin fining violators.

In conclusion, any mHealth developer or entrepreneur whose solution enhances the ability of the patient to interact with a provider may want to carefully consider the privacy and security requirements imposed on EHRs, and under HIPAA and other laws and regulations. Although the mHealth legal landscape is far from mature, there are significant risks of noncompliance with existing laws and guidance. No one wants to be that developer (and no one wants to be the investor in that developer) whose solution is targeted by the HHS, the FTC or any other governmental body for unlawful, or anti-patient/anti-consumer behavior, with possible fines and penalties. A governmental investigation or an enforcement action would likely be the death knell for a new mHealth product or service.

Lisa Clark practices in the area of healthcare law with emphasis on federal and state regulatory issues applicable to providers, HIPAA and privacy, managed care contracting, advertising and provider reimbursement, including through new delivery models such as pay for performance, shared savings and accountable care organizations (ACOs) and ACO-likes offered by commercial payors. Ms. Clark leads the firm's mHealth Multidisciplinary Team.

Disclaimer: This article is prepared and published for informational purposes only and should not be construed as legal advice. The views expressed in this article are those of the author and do not necessarily reflect the views of the author's law firm or its individual partners.

Note

1. "Patient Engagement Is the Holy Grail of Health Care," Steve Wilkins, M.P.H., *KevinMD.com*, January 27, 2012.

BY-LINED ARTICLE

Healthcare Reform and New mHealth Business Opportunities: What mHealth Entrepreneurs Should Know After the Presidential Election

By Mitch Goldman

November 14, 2012
mHealth Newsletter

mHealth investors and mHealth entrepreneurs may struggle to understand what business opportunities are present in the U.S. healthcare system since the passage of the Patient Protection and Affordable Care Act. Even if the Affordable Care Act is repealed or delayed, in whole or in part, it is likely that some of the initiatives under the law will move forward.

The Affordable Care Act has authorized the creation of new delivery models, a complex set of state and federal regulations, financial relationships and performance incentives. Many of the provisions of the Affordable Care Act offer mHealth entrepreneurs and investors new business opportunities and sources of revenue. Outlined below are some of these opportunities and markets that mHealth entrepreneurs and investors may want to consider:

- *Accountable Care Organizations (ACO)*. ACOs were prominently featured in the Affordable Care Act and have gained currency throughout the healthcare system. An ACO is an entity that consists of member hospitals, physicians (primary care and specialists), nursing homes, home healthcare providers and other ancillary providers. These providers are all collectively at-risk for delivering care to a population. The ACO contracts with an insurer for a global payment with incentives for better outcomes and lower costs. Instead of billing an insurer, the providers bill the ACO. All the providers are at risk for providing cost-effective, value-based care that is coordinated among the providers. Care coordination is one of the key values of the ACO that distinguishes it from health maintenance organizations (HMO) where there are no incentives for providers to do any care coordination. HMO providers are paid on a fee-for-service basis and are incentivized to provide more care. For the mHealth entrepreneur, there are numerous potential purchasers of mHealth apps, including member providers as well as the ACO. Both the ACO and all of its diverse provider members would value and pay for any mHealth app that promotes effective care coordination between and among healthcare providers, fosters positive consumer healthcare behavior and reduces the cost of delivering care.
- *Medical Home*. The medical home is a new delivery model for the care of patients with chronic illness that incorporates many of the key elements of the ACO—care coordination, pay for performance and collective risk assumption by all providers. Patients with chronic illness typically bounce from specialist to specialist for care, with no single professional or team of professionals managing care. The medical home is responsible for providing and coordinating all the care of a patient with a chronic illness such as diabetes. The captain of the medical home is a primary care physician, and all the other providers are at risk for the care of a patient. The medical home contracts for a capitated payment with an insurer or an ACO and pays its providers directly on a shared risk and pay-for-performance basis. The providers are paid to provide value-based, not volume-based, care. Similar to ACOs, the new entities and their member providers are likely to be a significant market for mHealth apps that improve care delivery, lower costs and further care coordination within a medical home.
- *Self-Funded Employers and Third-Party Administrators*. Companies that self-insure for their employees' health insurance also have an interest in reducing healthcare costs and can pay for new mHealth apps from their self-insurance trusts. However, most self-funded employers retain a claims manager, known as a third-party administrator (TPA), who manages the claims and provides other services to the self-funded employers, including negotiating discounted rates from healthcare provider networks. TPAs may also be a significant customer for mHealth apps that can potentially reduce healthcare costs by managing health claims from providers, improving employee health or making employees better purchasers. In addition, TPAs will likely have to redesign new payment models for providers to compete with the new approaches of ACOs and medical homes.

- *Health Insurance Exchanges*. Under the Affordable Care Act, states have the option to create electronic marketplaces for health insurance for individuals and small employers. Health insurers in each state will compete to offer four different types of plans. Consumers will purchase insurance through a portal. Similar to LendingTree, an individual would enter his or her specific data and receive several competitive insurance options. This new marketplace in each state will also offer mHealth app entrepreneurs new business opportunities from state agencies, vendors that develop the exchanges, insurers that participate in the exchanges and individuals and companies purchasing insurance policies.
- *Professional Liability Insurers*. While these insurers were not directly impacted by the Affordable Care Act, mHealth entrepreneurs should be aware that any mHealth app which improves the quality of care could be one that a professional liability insurer may want to buy or may want to offer a reduction in the insurance premium to the insured hospital or physician for purchasing the app. This could be an effective distribution channel for some mHealth apps.

The Affordable Care Act is likely to have a long-term impact on the healthcare system, potentially changing providers' and payers' behaviors. The new delivery models and the new government-supported programs appear to offer all mHealth entrepreneurs new business opportunities to improve healthcare quality, reduce cost and advance care coordination.

Mitch Goldman focuses his practice on the finance and corporate aspects of healthcare delivery, with an emphasis on reimbursement, structuring corporate transactions between and among providers, advising clients on the impact of government regulation, and developing and financing startup healthcare-related companies.

Disclaimer: This article is prepared and published for informational purposes only and should not be construed as legal advice. The views expressed in this article are those of the author and do not necessarily reflect the views of the author's law firm or its individual partners.

BY-LINED ARTICLE

mHealth and the FCC: What Does the FCC Have to Do with Medical Devices?

By Ken Keane

November 14, 2012
mHealth Newsletter

One might not associate the Federal Communications Commission (FCC) with mHealth issues. Yet, the FCC has a vital role to play in this field, and if recent developments are any indication, that role will likely grow.

On September 24, 2012, the FCC mHealth Task Force issued a report containing recommendations for FCC action on mHealth. The stated goal is that the FCC take action so that "by 2017 mHealth, wireless health and e-Care solutions will be routinely available as part of best practices for medical care."[1]

In a speech to the Information Technology & Innovation Foundation on the same day the Task Force recommendations were issued, FCC Chairman Julius Genachowski announced that the FCC will take the following actions to implement the Task Force's recommendations:

- First, the FCC will look to streamline its experimental licensing rules to encourage the creation of wireless health "test beds" to permit easier testing of mHealth devices.
- Second, the FCC will consider an order to reform the Rural Health Care Program. Among other things, this would permit networks of hospitals and healthcare facilities to jointly apply for program funds in order to boost broadband capacity and enable electronic health records.
- Third, the FCC will encourage regulators in other countries to make spectrum available for a new type of device, Medical Body Area Networks (MBANs), and discuss possible spectrum harmonization for these devices. This would allow for patient travel and better economies of scale for device makers.
- Fourth, the FCC will develop an outreach plan to promote collaboration between the FCC and the healthcare sector on communications policies.
- Fifth, Chairman Genachowski said that the FCC would recruit a permanent Healthcare Director who would function as the agency's point of contact on all health-related issues.

FCC action in the healthcare field is by no means new for the agency. The Commission has long sought to provide spectrum resources to support wireless medical technology. For example, the agency has allocated spectrum for the Wireless Medical Telemetry Service (WMTS). By means of WMTS devices, patient information can be transmitted wirelessly within a hospital and to other locations.

Likewise, in 2010, the Commission finalized a memorandum of understanding (MOU) with the U.S. Food and Drug Administration for collaboration between the two agencies. This is noteworthy given the jurisdictional overlap: The FCC has statutory authority over devices that emit radio energy, and the FDA reviews and approves medical devices for patient safety and medical efficacy. The two agencies agreed on the following principles:

- Developing and integrating wireless and broadband communications technologies with medical devices and applications, which requires agencies to assure that such devices operate in a safe, reliable and secure manner.
- It is essential for the federal government to provide leadership and encourage innovation and investment in new healthcare technologies that enable patients, doctors and other health professionals to access the highest-quality care.
- The American public—including industry, providers, patients and other interested stakeholders—should have clear regulatory pathways, processes and standards to bring broadband and wireless-enabled medical devices to market.

Since adoption of the MOU, the FCC has continued to be proactive in the wireless medical device field. In 2011, the FCC adopted rules to enable a new generation of wireless medical devices that can be used to restore functions to paralyzed limbs. Medical Micropower Networks (MMNs) are ultra-low-power wideband networks consisting of transmitters implanted in the body that take the place of damaged nerves, restoring sensation and mobility.

As FCC Chairman Genachowski said, these networks "have the potential—literally—to enable paraplegics to stand and to restore sight to the blind."

In May 2012, the FCC adopted rules for the aforementioned MBANs, which has enabled the United States to become the first country in the world to allocate spectrum for these types of devices. MBANs units will provide a cost-effective way to monitor patients wirelessly, providing more information to physicians and giving patients mobility and greater independence.[2]

In short, the FCC—while not an agency that one would immediately think of as being involved in mHealth issues—has a vital role to play in this rapidly expanding field. That role will likely grow with the continued development of wireless medical technology.

William K. (Ken) Keane practices in the area of telecommunications law and policy. His practice focuses on the representation of clients in radio spectrum policy and transactional matters. For example, he counsels broadcast and industrial clients on FCC compliance issues; prepares license applications and other filings for submission to the Commission; represents clients in FCC enforcement proceedings; and provides advice and counsel in connection with communications asset transactions.

Disclaimer: This article is prepared and published for informational purposes only and should not be construed as legal advice. The views expressed in this article are those of the author and do not necessarily reflect the views of the author's law firm or its individual partners.

Notes

1. mHealth Task Force Findings and Recommendations, Pre-Publication Public Draft, September 24, 2012, at page 1.
2. Duane Morris played an active role in the formulation of the FCC rules governing MBANs devices, which rules remain subject to reconsideration by the agency.

BY-LINED ARTICLE

mHealth and Home Health: A Natural Fit

By Mark J. Silberman

November 14, 2012
mHealth Newsletter

Home health is an industry built on the core value of having hands-on-professionals providing quality healthcare in the comfort and privacy of the patient's home. The availability of reliable data is particularly key in home health, since the patient and his or her caregivers are not always in the same location as compared to a hospital or nursing home. When the caregiver is in the home, the information collected through patient assessments must be accurate and has to circulate back to the patient's physician and other caregivers as promptly as possible to determine and maintain optimum treatment. The patient can also benefit when caregivers share information with him or her about the treatment plan, including how the patient can be an active participant in his or her healthcare. Good data are thus necessary in home health to effect good outcomes and to engage the patient in his or her care experience.

mHealth software applications and devices provide the ideal tools to advance home healthcare through the prompt and targeted exchange of patient data. Numerous apps on smart phones, tablets and laptops, as well as stand-alone devices, can provide real-time information to healthcare professionals to monitor a patient's heart rate, blood pressure, sleep, blood oxygen levels, glucose levels and coagulation. A sample mHealth product that relies on a smartphone (or other platform) may include an accessory, such as a stethoscope, that is connected to the smartphone and a mHealth app that allows data to be collected through the accessory and sent to a provider. When the stethoscope is held up to the patient's heart area, it can detect beats-per-second and then transmit the data through the app. The provider that receives the data can then use the data to monitor the patient's health and can share the information with other providers through an electronic health record or other means in order to determine treatment.

Less-complex mHealth apps exist that, for instance, can remind the patient to take his or her medicine with the use of a ringtone. The patient must then confirm through the app, such as by pressing a button on a touchscreen, that he or she has taken the medicine, along with the time. Other apps allow the patient at home to transmit to the physician real-time information on signs and symptoms—such as an emerging rash—via text, photo or video message. Finally, apps are available that educate the patient on healthy lifestyles and specific care instructions, such as how to clean a simple wound.

Concerns have been raised on whether mHealth devices and apps, especially those that support monitoring, diagnosis or clinical-care decision making, will cause home health to forego, or at least drastically minimize, the hands-on touch. The industry will have to find the right balance of providing care through technology and with flesh-and-blood professionals. Some of the clinical, legal and financial issues to consider are:

- What standards of care will apply to the provision of care through mHealth? How will the licensing and accrediting agencies view mHealth? Is the provision of care through mHealth equivalent to the practice of medicine?
- Which aspects of mobile health, *i.e.*, the devices, applications and/or accessories or combinations thereof, will be reimbursable by the government and private insurers? If not reimbursable, who will pay (*e.g.*, would the patient or the provider have to subscribe to a particular app).
- How will the industry deal with the inherent risks and liabilities related to the electronic transmission of data? Who will ensure that the data are protected and properly transmitted (*e.g.*, if your patient's network goes down or an alert from the monitoring device gets caught in your spam filter)? Depending on how data are transmitted, what is the role of the hosting company or other vendors engaged in the collection, storage and transmission process?
- How will the government regulate mHealth?

With respect to government oversight, a number of agencies have their hands in the pot. The Food and Drug Administration is developing guidance for regulating mHealth devices, including apps and other software. The Department of Health and Human Services is considering mHealth and privacy issues. The Federal Trade Commission is closely watching the entire mobile app industry to ensure that apps are properly advertised and that the intended uses of the data are transparent to the user. Congress has also weighed in, requiring the agencies to develop an overall regulatory framework for mHealth.

A natural fit exists between home health and mobile health, given that, except for home visits and doctor's visits, patients and providers are not in the same place. mHealth is likely to continue to prove its value in the home health sector and aligns with anticipated changes in the U.S. healthcare system. The utilization of real-time monitoring devices in the home can assist in avoiding acute episodes, thereby reducing readmissions, a current high-level concern under Medicare. The ability to deliver care remotely and encourage patient engagement is likely to be attractive to accountable care organizations and other healthcare initiatives that are designed to reduce costs in the healthcare system. The advantages to the use of mHealth in home health are apparent—if issues like reimbursement and applicable laws can be resolved.

Mark J. Silberman practices in the area of health law. His practice focuses upon governmental and regulatory compliance in healthcare, with concentrations in healthcare litigation, healthcare-related white-collar criminal defense and all aspects of the Illinois Certificate of Need program. Mr. Silberman handles compliance and enforcement actions involving the Illinois Department of Public Health, Illinois Health Facilities and Services Review Board (formerly Health Facilities Planning Board) and Medicare/Medicaid programs. He also advises clients regarding pharmacy and pharmaceutical-related litigation, Stark laws, HIPAA, allegations of healthcare fraud and healthcare-related criminal conduct.

Disclaimer: This article is prepared and published for informational purposes only and should not be construed as legal advice. The views expressed in this article are those of the author and do not necessarily reflect the views of the author's law firm or its individual partners.

BY-LINED ARTICLE

AliveCor Veterinary ECG Model Paves FDA-Friendly Path to the Market

By Michael A. Swit

November 14, 2012
mHealth Newsletter

In a recent move that mobile medical application developers may want to emulate, AliveCor—the developer of a mobile electrocardiogram (ECG) system awaiting U.S. Food and Drug Administration (FDA) blessing for human use—has introduced what appears to be essentially the identical product for the veterinary market, and without getting FDA's permission.

AliveCor's strategy takes advantage of what might be considered a gap in FDA's regulatory regime. Specifically, medical devices labeled solely for veterinary use do not require any type of prior clearance or approval by the FDA. While such devices still must be properly labeled and also manufactured under appropriate quality conditions, the agency lacks specific statutory authority to require submission of anything resembling a pre-market notification submission [510(k)] or Premarket Approval Application (PMA) as might be required for an identical device intended for human use.

mHealth medical device innovators interested in pursuing this veterinary approach should keep in mind that the absence of a need for FDA approval or clearance does not eliminate the need to have adequate substantiation for any claims made about a product's effectiveness or safety in the species targeted for the product. Inherent in FDA's statutory authority to prevent the marketing of adulterated or misbranded devices is the power to probe the adequacy of the substantiation of labeling claims. In addition, depending on how the product is marketed, concurrent jurisdiction may exist between FDA and the Federal Trade Commission (FTC). The FTC also expects marketers to have appropriate substantiation for product claims.

AliveCor's strategy of pursuing a veterinary medicine use, even pending FDA clearance of its human model, is a creative development in the mHealth arena. However, while FDA preclearance is not required, care should be exercised in pursuing an animal health use for a mHealth product, including not only ensuring adequate substantiation of label claims, but also conforming to FDA's general regulations applicable to veterinary medicine devices. Regardless of whether it is subject to FDA preclearance, developers should incorporate appropriate risk-management steps to maximize the safety and efficacy of any product that impacts human or animal health.

Michael A. Swit's practice focuses on solving the legal challenges confronted by the pharmaceutical, medical device, and other life sciences industries in tackling the myriad of legal mandates enforced by the U.S. Food & Drug Administration. Mr. Swit has extensive experience counseling life sciences firms on the demands of compliance with FDA's statutory and regulatory requirements to develop and market safe and effective drugs, biologics, medical devices, IVDs and other products.

Disclaimer: This article is prepared and published for informational purposes only and should not be construed as legal advice. The views expressed in this article are those of the author and do not necessarily reflect the views of the author's law firm or its individual partners.