The OCR's recent guidance for mHealth app developers

The US Department of Health and Human Services Office for Civil Rights ('OCR'), which monitors Health Insurance Portability and Accountability Act 1996 ('HIPAA') violations, plays a crucial role in monitoring mHealth apps used by healthcare providers. Recently the OCR issued guidance for mHealth app developers, which is intended to assist those developers in determining the applicability of HIPAA to them. Sheryl Tatar Dacso, Partner at Seyfarth Shaw LLP, and member of the *eHealth Law & Policy* editorial board, discusses the context and details of the OCR's guidance.

The development of new technologies to transmit and receive health information using wireless systems has launched a rapidly growing industry referred to as 'mHealth.' These new channels of communication involve data and information affecting healthcare services as well as medical devices. This disruptive technology has been used extensively in other industries and is now expanding rapidly in the healthcare space. mHealth products and services can be in the form of a mobile app, or can be web-based or desktop. For example, wearable devices, healthcare services and support, Personal Health Record ('PHR') and Electronic Health Record ('EHR') access, hospital survey tools and clinical decision support bring the consumer and providers into new relationships and have raised new issues associated with the use of this technology. The storage and wireless transmission of protected health information ('PHI') to and from mobile devices means that the HIPAA Privacy Rule and Security Rule will affect covered entities ('CE') and business associates ('BA') using such devices. Those who are developing mobile applications ('apps') have been challenged by ambiguity in the HIPAA law, which can affect not only the user of the device but also the developers of the app associated with the device. Those used by healthcare providers perform a wide range of functions, including storing patient information and reviewing lab results[1]. These apps are often integrated into other technology systems such as cardiac monitoring devices. Apps used by consumers outside of the healthcare system are private apps. Apps in this category include, for example, fitness apps that measure calories consumed and weight loss and apps that contain information on diseases and symptoms.

The development and use of apps in healthcare are subject to policies and laws including those related to medical licensure to privacy and security protection, as well as legal liability. Because the app may deal with information that is a PHR or EHR, it is important to consider whether it is created or maintained by a CE or a BA as official medical records (EHR) or is merely medical information that is consumer-facing and not necessarily part of a patient's medical file (PHR). The former is a medical record of the provider intended to facilitate treatment and the latter is health information that informs the patient.

Five federal agencies directly or indirectly regulate health apps: the National Institute of Standards and Technology ('NIST'), the Federal Communications Commission ('FCC'), the Office for Civil Rights of the Department of Health and Human Services ('HHS'), the Federal Trade Commission ('FTC'), and the Food and Drug Administration ('FDA')[2]. Although the NIST is a non-regulatory body, it is likely to affect the development of apps in the form of guidance standards for mobile and software technology. The FCC has not yet exerted jurisdiction but has the capacity to authorise carriers to access, transmit, and store information from devices connected to their networks. The HHS OCR, which monitors HIPAA violations, already plays a crucial role in monitoring of health apps used by care providers. The FTC regulates false and deceptive advertising. It has already brought enforcement proceedings against developers of private health apps based on a focus on consumer protection[3]. These agencies have weighed in on this growing industry based on the particular application involved and its intended use. The FDA has authority to regulate medical devices through section 201(h) of the Food, Drug, and Cosmetic Act 1938 and the Medical Device Amendments of 1976 to that Act. The Agency has indicated that it will use its authority to regulate only mobile medical apps "whose functionality could pose a risk to a patient's safety if the mobile app were to not function as intended."[4]

In an effort to bring some clarity to the many questions being raised by app developers, the OCR issued guidance on 11 February 2016 that sought to explain the application to the use of apps. The guidance document published by the OCR on its mHealth Portal is intended to help app developers determine the applicability of HIPAA to them as a BA, based on their role in the access, use and storage of data associated with the app[5]. A BA is defined as a service provider for a CE if it receives, maintains, or transmits PHI on behalf of a CE[6].

In developing this guidance, the

OCR based its scenarios around two questions:

1. 'How does HIPAA apply to health information that a patient creates, manages or organizes through the use of a health app?' To determine if you are a BA, ask the following questions:

- Does your health app create, receive, maintain, or transmit identifiable information?
- Who are your clients? How are you funded?
- Are your clients covered entities? (e.g. hospitals, doctor's offices, clinics, pharmacies, or other health care providers who conduct electronic transactions; health insurance issuers; health or wellness programme related to a health plan offered by an employer).
- Were you hired by, or are you paid for your service or product by, a covered entity? Or another business contracted to a covered entity?
- Does a covered entity (or a business associate acting on its behalf) direct you to create, receive, maintain or disclose information related to a patient or health plan member?'

and

2. 'When might an app developer need to comply with the HIPAA Rules?'

An app developer is NOT subject to HIPAA if the developer is not engaged by the CE or BA to create, maintain or transmit PHI on behalf of a CE or BA. However, if a CE or BA contacts with an app developer for patient management and the patient is instructed to download and use the app, HIPAA will apply. In summary, health apps that are downloaded and used solely by the consumer do not implicate HIPAA even if (1) the provider recommends the health app, (2) the consumer uploads or downloads PHI to the app, or (3) the app developer has an interoperability agreement with the provider allowing transmission to the provider. The key consideration by the OCR for BA status is in determining who creates, receives, maintains and transmits PHI in relationship to CEs or other BAs.

In an effort to bring some clarity to the many questions being raised by app developers, the OCR issued guidance on 11 February 2016 that sought to explain the application to the use of apps

Sheryl Tatar Dacso Partner
Seyfarth Shaw LLP, Los Angeles and Houston
SDacso@seyfarth.com

1. Melnik T. 'Mobile tech: is it right for your organization?' J Health Care Compliance. 2011;13(6):49–52.
2. Washington L. 'Managing health information in mobile devices.' J AHIMA. 2012;83(7):58–60.
3. See Dolan B, Gullo C. US regulators remove two acne medical apps. MobiHealthNews [serial on the internet]. 9 September 2011 [cited 2 January 2014]. Available from: http://mobihealthnews.com/13123/us-regulators-remove-two-acne-medical-apps and Federal Trade Commission. Peer-to-peer file sharing: a guide for business [Internet]. Washington (DC): FTC; [cited 2 January 2014]. Available from: http://www.business.ftc.gov/sites/default/files/pdf/bus46-peer-peer-file-sharing-guide-business.pdf
4. Food and Drug Administration. Mobile medical applications: guidance for industry and Food and Drug Administration staff [Internet]. Silver Spring (MD): FDA; 25 September 2013 [cited 3 January 2014]. Available from: http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf
5. See http://HIPAAQsportal.hhs.gov. This guidance follows OCR's release last fall of a 'developer portal,' a platform linked to the OCR privacy site [http://www.hhs.gov/hipaa/index.html] that enables mobile health developers and others to get a better understanding of how HIPAA regulations apply to new technologies.
6. Business Associate: (1) Except as provided in paragraph (2) of this definition, business associate means, with respect to a covered entity, a person who: (i) On behalf of such covered entity or of an organized health care arrangement (as defined in §164.501 of this subchapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of: (A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or (B) Any other function or activity regulated by this subchapter; or (ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in §164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person. (2) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health care arrangement. (3) A covered entity may be a business associate of another covered entity. Serwin, Information Security and Privacy, §30:1 (West 2015), citing 45 C.F.R. §160.103.