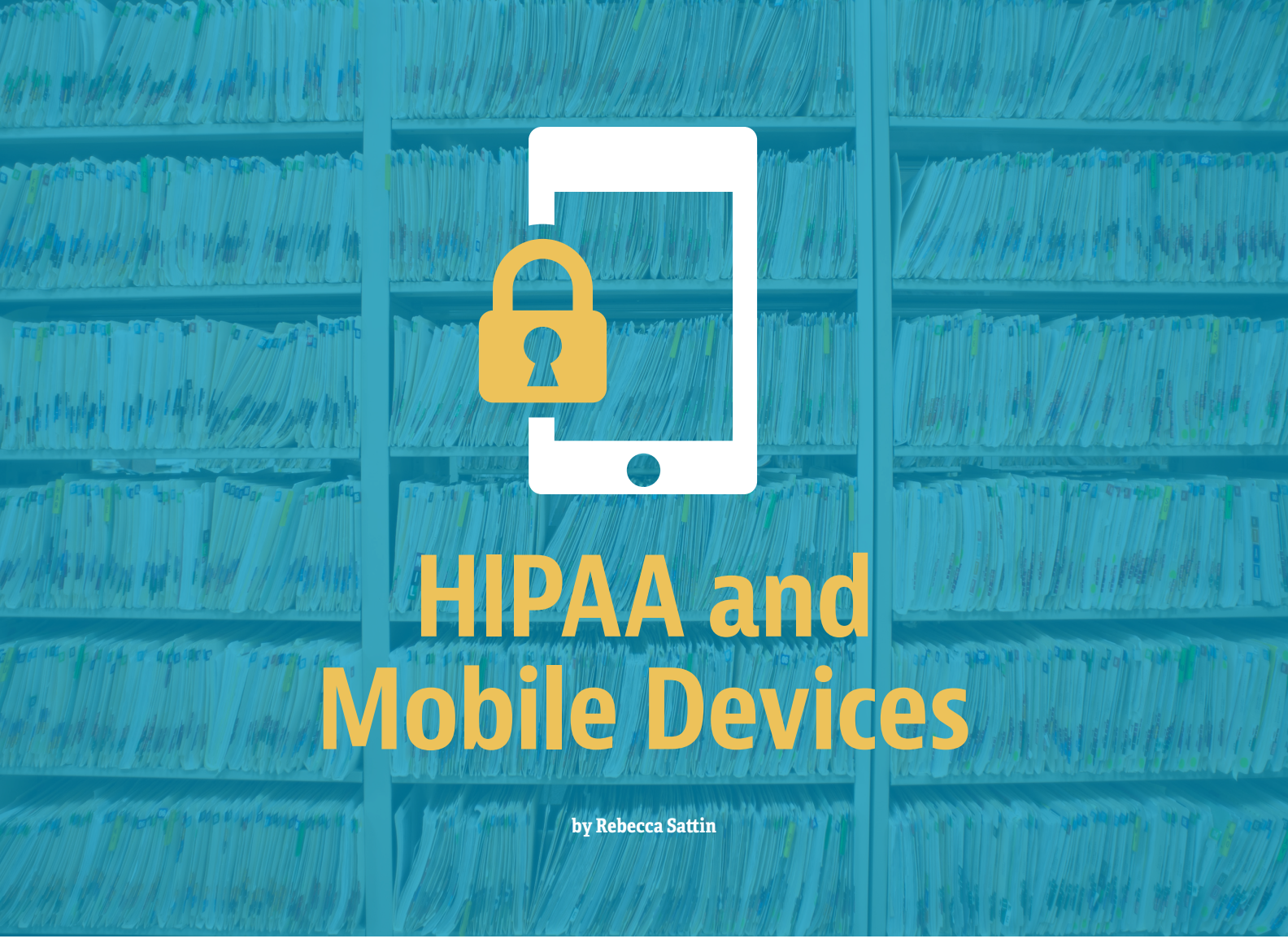

HIPAA and Mobile Devices

by Rebecca Sattin

If your law firm works primarily with health care providers, then you already know about the Health Insurance Portability and Accountability Act (HIPAA) and its requirements. For those firms that only occasionally encounter health care providers, it is helpful to understand what may be required to protect client data, especially for mobile devices.

Covered Entities and Business Associates

HIPAA defines a "covered entity" as "a health plan, a health care clearinghouse or a health care provider who transmits any health information in electronic form..." [§ 160.102 (a)]. Law firms typically are not covered entities unless they are large enough to administer their own health plans. Instead, they are more often business associates of covered entities. A "business associate" "provides legal,...consulting, data aggregation management,...administrative...or financial services to or for such covered entity...where the provision of the service involves the disclosure of protected health information from such covered entity...or from another business associate of such covered entity...to the person" [§ 160.103].

It is when they act in this capacity that law firms encounter HIPAA compliance issues. Law firm vendors processing client data would also be acting as business associates and be subject to the same compliance issues. As of 2013, business associates of covered entities are directly liable for compliance with some provisions of HIPAA when in possession of a client's electronic Protected Health Information (ePHI).

Several provisions, called safeguards, need to be considered when deciding how to manage the proliferation of mobile devices at law firms and which apps should be allowed. The safeguards fall into three categories: administrative, physical and technical. Here are some of the administrative and technical safeguards to consider.

Administrative Safeguards

One of the administrative safeguards that affects all technology, mobile devices included, is that risk management and sanction policies must be in place to evaluate and implement new technology or systems. Mobile device management policies should be crafted with this in mind. Each new strategy or app should be evaluated with an eye toward assessing and mitigating risks as specified in the firm's policy.

Another administrative safeguard instructs organizations to have a defined procedure for terminating access to ePHI when employment ends. This safeguard is listed as "addressable" rather than "required," meaning the covered entity or business associate must assess whether the specification is reasonable and appropriate for the organization to implement. With law firms, this will almost always be appropriate. For mobile device policies, there are several ways to handle this safeguard.

» Firms that use containerized solutions can wipe firm data from the device, leaving personal data in place.

» Another option is to have a policy requiring employees using personal mobile devices to consent upfront to a device wipe upon leaving the firm.

When evaluating individual mobile device apps, find out if data accessed within the app is stored on the device and, if so, whether the data can be accessed once credentials have been revoked. Pay close attention to apps and browser-based products that allow sharing and transferring of documents to people both inside and outside the firm. Also beware of cloud backup services associated with the various mobile device brands. These should be disabled since firms do not want their data replicating to any services outside their control or being restored to devices following device wipes.

Technical Safeguards

The encryption standards outlined in the HIPAA technical safeguards are specified as addressable; if firms deem encrypting data as not reasonable or appropriate, they must document why and implement an equivalent alternative measure. Setting up encryption for mobile devices and apps is relatively simple, since management software from Microsoft's ActiveSync to the more granular third-party products can specify that device enrollment is contingent upon device encryption being enabled and complex passwords being set.

The more elusive goal is ensuring that transmitted data are encrypted. When an email message is sent from a mobile device, the message may be encrypted between the device and the firm's email server; but, unless the firm has other products or features in place, the message is not encrypted once it exits the firm's server. Health care clients should be reminded never to send ePHI either in the body of an unencrypted email message or as an unencrypted attachment.

One of the safeguards that falls across all three categories is the need for a clearance process — unique user access authorization, control and validation for access to ePHI. This safeguard restricts access to ePHI to the fewest number of people needing it to perform the service. Each user must have his or her own account and authentication to access it, with automatic logoffs for session termination and inactivity timeouts. Based upon their risk assessment, each firm can determine the period of inactivity that will trigger the timeout. Short inactivity timeouts might not be popular, so they can be implemented only for those who have access to ePHI.

Review and Protect

There are many mobile device apps that allow access to firm data. Some DMS products have apps or browser-based methods for accessing documents; litigation support products often have browser-based methods or apps for document review or transcript management. As before, strong passwords and timeouts should be in place to prevent unauthorized access, and apps should be evaluated to determine whether any data viewed within the app or browser are retained on the device, even if only temporarily.

When acting as a business associate to a covered entity, the best way to prevent compliance issues is not to transmit or store any of the client's PHI on your system. If only this were always possible! Since it is not, firms must enact and enforce policies that extend their security and access control from their internal systems to mobile devices. Understanding the way mobile applications store and transmit data and their behavior when access is revoked is critical when evaluating new apps or browser-based products accessible from mobile devices. **P2P**

REBECCA SATTIN
Rebecca Sattin joined World Software Corporation in August of 2015 as CIO. She was formerly at Mitchell Silberberg & Knupp LLP for 18 years, where she was the director of information technology. She has more than 20 years of experience in the area of law firm technology. Contact Rebecca at rsattin@worldox.com.

This article was first published in ILTA's Spring 2016 issue of Peer to Peer titled "There's an App for That!" and is reprinted here with permission. For more information about ILTA, visit www.iltanet.org.