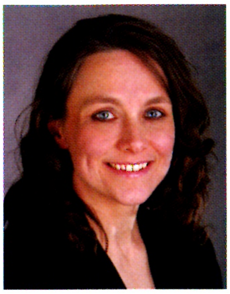

Securing Health Information on Mobile Devices

By Joy D. Kosiewicz

THE PROLIFERATION OF electronic media and mobile devices creates a challenge for providers to maintain security over their patients' electronic protected health information (ePHI). Lost and stolen mobile devices account for most of the recent HIPAA breach settlements involving the Department of Health and Human Services (HHS). Further, HHS will be carefully reviewing provider risk assessments and mobile device policies as the HIPAA Audit Program is fully implemented this year.

Addressing all of the security risks associated with mobile devices may seem daunting. However, a review of recent HHS enforcement activity and guidance will assist providers with prioritizing compliance efforts. The Resolution Agreements resulting from the HIPAA breach settlements offer guidance on what providers must do to secure mobile devices in compliance with the HIPAA Security Standards for the Protection of Electronic Protected Health Information. HHS has also issued new tools to assist providers with protecting ePHI that may be accessed, created, stored or transmitted on mobile devices.

The first step every provider must take is to conduct a risk assessment that identifies all mobile devices that contain or are used to access, create, store or transmit ePHI. This includes devices owned by the provider and personal devices used by the provider's workforce members. The risk assessment should be conducted at least annually, and more frequently as necessary, to address changes in internal policies.

Once all mobile devices are accounted for, providers must assess potential risks in using the mobile devices and decide what security measures will be used to address those risks. Initially, providers should consider to what extent they want to permit the use of ePHI on company-owned or personal mobile devices and how they will control such use.

The next step is to develop policies and procedures that implement the security measures and set standards for the workforce. Policies and procedures need to address at least all of the following:

+ Proper uses and disclosures of ePHI through mobile devices
+ Authorization and restriction of access to ePHI through mobile devices
+ Reasonable means of tracking mobile devices containing ePHI in and out of, and within, provider's facility
+ Identification, reporting, and responding to security incidents and breaches, including mitigation plans
+ Encryption and decryption of mobile devices, or an equivalent alternative to encryption that includes the rationale supporting the decision not to use encryption
+ Disposal and re-use of mobile devices
+ Training of provider's workforce on the use and security of mobile devices
+ Sanctions for failure to comply with the policies and procedures

It is important that the provider document risk assessment, training sessions and any actions taken in response to a breach or potential breach. This type of documentation, along with the provider's policies and procedures, will be requested during a HIPAA audit.

Mobile devices require the same security protections providers implement with health information maintained on paper and other electronic media. The key is being able to identify, track and control how ePHI is accessed, maintained and transmitted on mobile devices.

Joy Kosiewicz is Partner of the Health Care Practice Group of Brouse McDowell in Akron.