eALERT

INCompliance

December 18, 2012

New HIPAA Tools for Mobile Devices

On December 12, 2012, the Department of Health and Human Services (HHS) launched a new education initiative and set of online tools to offer health care providers practical tips on ways to safeguard protected health information when using mobile devices such as laptops, tablets and smartphones.

The initiative is called "Mobile Devices: Know the RISKS. Take the STEPS. PROTECT and SECURE Health Information" and is available at: www.HealthIT.gov/mobiledevices. The website offers educational resources such as videos, fact sheets and posters with recommendations on how to safeguard protected health information.

The initiative materials advise taking the following steps to secure protected health information on mobile devices:

1. Use a password or other user authentication
2. Install and enable encryption
3. Install and activate remote wiping and/or remote disabling
4. Disable and do not install or use file sharing applications
5. Install and enable a firewall
6. Install and enable security software
7. Keep your security software up to date
8. Research mobile applications before downloading
9. Maintain physical control (i.e., protect against lost devices)
10. Use adequate security to send or receive health information over public Wi-Fi networks
11. Delete all stored health information before discarding or reusing the mobile device

HHS notes that while there has been a proliferation of mobile devices in the health care setting, a recent survey indicated that only 44 percent of survey respondents encrypt their mobile devices.

Lost laptops and other mobile devices continue to be one of the most significant HIPAA security risks and account for many of the large HIPAA breaches and penalties. Within the past few months alone a provider paid a $1.5 million penalty for a lost laptop containing unencrypted protected health information and a state health agency paid a $1.7 million penalty for a lost USB drive containing unencrypted protected health information.

Covered entities and business associates need to take steps to review their security policies and protocols regarding mobile devices. Covered entities and business associates should review how protected health information is stored on and accessed by mobile devices and ensure that those mobile devices will maintain the security of the protected health information.

This eAlert was prepared by Allen Killworth (614) 227-2334 or akillworth@incomplianceconsulting.com. Please contact any INCompliance consultant for more information at info@incomplianceconsulting.com.