C. Scott Litch
Chief Operating Officer and General Counsel

Litch's Law Log

Protecting Patient Health Information on Mobile Devices

Mobile device use seems to keep increasing exponentially, and health care is no exception. While the HIPAA privacy law applies to any dental practice that sends patient information electronically (such as insurance claims submissions), HIPAA does not prohibit the use of mobile devices to send patient health information. HIPAA does require implementation of reasonable safeguards to limit incidental uses or disclosures of patient information that may result from any use or disclosure permitted under HIPAA. Therefore, a number of precautionary steps are recommended. The federal government website *www.HealthIT.gov* provides the following 11 useful tips concerning mobile devices.

"Use a password or other user authentication.

You can configure your mobile device to require a password, personal identification number (PIN), or passcode (a pattern you trace with your finger) to gain access to the device. Keep your password, PIN, or passcode a secret, and don't store them on your mobile device. You can also configure your mobile device to automatically lock or log you off after a set time of inactivity.

Install and enable encryption.

Encryption is the conversion of data into a form that cannot be read without the decryption key or password. It is important to encrypt data stored locally on your mobile device (data at rest) and data sent by your mobile device (data in motion) so that it is protected from unauthorized users.

Install and activate wiping and/or remote disabling.

Remote wiping is a security feature that enables you to remotely erase the data on the mobile device if the device is lost or stolen. When you enable remote wipe feature on your mobile device, you have the ability to permanently delete data stored on your lost or stolen mobile device.

Remote disabling is a security feature that enables you to remotely lock or completely erase data stored on a mobile device if it is lost or stolen. If the mobile device is recovered, it may be unlocked.

Disable and do not install or use file sharing applications.

File sharing is software or a system that allows individual users of the Internet to connect to each other and trade fi s.

Install and enable a firewall.

A personal fi ewall can protect against unauthorized connections by intercepting incoming and outgoing connection attempts and blocking or permitting them based on a set of rules.

Install and enable security software.

Security software protects against malicious software such as viruses, spam and malware. A virus is a self-replicating program that runs and spreads by modifying other programs or files. Spam is the abuse of electronic messaging systems. It is electronic junk mail. Malware is a program that is inserted into the operating system of a mobile device, to compromise the confidentiality, integrity, or availability of the data, application, or operating system of the device. This is usually done covertly without the user's awareness.

Keep your security software up to date.

Security risks and threats are changing rapidly. By updating your security software you know that you have the latest tools to prevent unauthorized access to health information on your mobile device.

Research mobile applications (apps) before downloading.

A mobile app is a software program for mobile devices. Some examples of mobile device apps are games, note taking programs, research programs, and health related tools, such as EHR software.

Maintain physical control.

Mobile devices are easily lost or stolen due to their small size and portability. A mobile device that is accessible to unauthorized users poses a risk to the confidentiality, integrity, and availability of health information on the mobile device. If you physically secure your mobile device, you can limit the risk of unauthorized users tampering with or stealing it.

Use adequate security to send or receive health information over public Wi-Fi networks.

Wi-Fi stands for Wireless Fidelity. It refers to wireless data networking technologies. Wireless data networking links computers, including mobile devices, without wires (such as an Internet cord). The risk of using a public Wi-Fi network (or hotspot) is that information can be intercepted between the mobile device and the system connection.

Delete all stored health information before discarding or reusing the mobile device.

By using software tools that thoroughly delete (or wipe) health information stored on a mobile device before discarding or reusing it, you can protect and secure the information from unauthorized access."

More details can be accessed on the *www.HealthIT.gov* website at *https://www.healthit.gov/providers-professionals/how-can-you-protect-and-secure-health-information-when-using-mobile-device.*

Readers may also be interested in the following article, which provides additional considerations for dental offices: *http://www.dentalproductsreport.com/dental/article/hipaa-compliance-and-digital-photography-personal-mobile-devices.*

For further information contact Chief Operating Officer and General Counsel C. Scott Litch at (312) 337-2169 ext. 29, or *slitch@aapd.org.*

This column presents a general informational overview of legal issues. It is intended as general guidance rather than legal advice. It is not a substitute for consultation with your own attorney concerning specific circumstances in your dental practice. Mr. Litch does not provide legal representation to individual AAPD members.