HIPAA and Electronic Communication/Texting: Suggestions from the Board

Cell phone texting and E-mail communication has been increasing among physicians and athletic trainers. The use of these technologies has made it more feasible for the health care team to communicate and become more efficient in the delivery of health care to patients. In fact, in many cases this is often a preferred way of exchanging orders and discussing injuries in real time when making decisions regarding participation and or treatment paths. For example, discussing results of laboratory tests, interpretation of those results and anatomic Radiology reports [e.g., X-ray and MRI reports] can have real time implications for patient's participation decisions. Most patients and their family members are likely to want this information as soon as possible, via the most rapid, efficient, and effective mode of communication. Health care professionals need to receive the information rapidly to manage patient care. Clearly, texting and e-mail communication facilitates care. However, with this mode of communication is the ability to send protected health information (PHI), securely, confidentially, and privately, such that only the intended recipient(s) is (are) privy to the content of a text or e-mail containing PHI.

In 2013, the government set forth an electronic communication update to the previous legislation in the Health Insurance Portability and Accountability Act 1996 (HIPAA). This was done in order to increase the security of patient health information through these means of transmission. The new HIPAA policy was introduced to eliminate the risk of patient health information being compromised during the sending or receiving of sensitive data via email, or SMS, or while patient health information is kept on a portable mobile device (cell phone, tablet, Smartphone, etc.).

There is increased concern about access to protected information being shared through portable mobile devices. There is clearly a potential for patient data security breaches as Athletic trainers are using email, or SMS, via portable mobile device to communicate information to colleagues or share information with their team physicians about their patients.

Issues to consider:

The revised HIPAA policy accounts for the lack of security on many portable mobile devices, and the fact that few portable mobile device owners use passwords to protect sensitive patient health information stored on them.

The new HIPAA guidelines also address sensitive patient health information that is transmitted by text to or from personal portable mobile devices, which is not encrypted and which should now be deleted if no encryption security measure is in place.

New HIPAA texting rules have also been introduced to safeguard patient health information when it is sent, received or reviewed, by the portable mobile device owner over an unsecured cellular network or public Wi-Fi.

HIPAA rules “require appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information”.

What does this mean to you?

You need to work with your employer to determine how these new HIPAA rules affect you. Make sure you discuss with them how you communicate PHI, how you are controlling who has access to patient health information, how that information is transmitted and received, and how it is consequently protected when it is stored on a portable mobile device. They should be able to help you with protocols for these types of communication. Even if HIPAA doesn’t directly impact your facility or practice location these can be seen as best practices for athletic trainers in all settings.