Smartphones aren't so HIPAA Smart!

HIPAA violations due to cell phone use are becoming a common problem, and we are finding ourselves left with "smartphones" that are HIPAA-dumb. Staff members and even physicians are not always as careful as they should be, while those of us acting as auditors, compliance professionals, and consultants often receive medical records via email, which is then delivered to our phones or other handheld devices.

Passwords are annoying and can be a challenge with our cell phones, but not having a password (and a password that meets acceptable standards as opposed to "spacebar") not only leaves your device vulnerable, but leaves you personally responsible for protecting the integrity of the PHI. Furthermore, sending PHI to another covered entity by text or email retrieved by phone is not as safe as you would think.

We commonly see disclaimers on emails and messages that say "consider your environment when reviewing this message," but how many of us truly pay attention? If you are in an elevator and view an email or text that may have PHI, the person standing next to you may be looking at your phone. Please consider the consequences when sending PHI to anyone. Encrypted texts and emails may provide some protection, but if someone wants that information badly enough and knows how to get it, they can.

Take these steps to protect you and the organization you represent.

1. 1. **Warn about safety in a disclaimer.** Provide a disclosure that states that the method of communication that is being used may not be safe, and it is the reader's choice to respond by the same method or to use a more compliant manner to continue the conversation.
2. 2. **Warn about unauthorized viewing.** Include a disclosure that if the email is seen by anyone other than who it was intended for, those who view it accidentally should destroy the information immediately to avoid any HIPAA violation. The warning should also state that using the information could result in large fines and possible jail time. At minimum, this demonstrates your efforts to ensure compliance with noted PHI.
3. 3. **Avoid voicemails to general mailboxes.** Do not leave a voicemail messages that could be retrieved or intercepted by anyone other than your intended recipient. Keep the information in your recording to a minimum and make it more ambiguous than a normal discussion with the patient. Note that many people are using VOIP systems such as Google Talk these days. Such services can be set to automatically transcribe voicemails and send them to the individual via email and/or text - leading to a potentially unforeseen HIPAA exposure. The big picture with HIPAA is to guard yourself, guard the PHI, and be on the offensive as well as the defensive regarding information that you send and receive.

Kelly D. Ogle, MSOP, BSDH, is an OSHA and HIPAA Compliance Specialist
Kelly D. Ogle is an OSHA and HIPAA Specialist for DoctorsManagement. Kelly provides OSHA and HIPAA training and consulting to help medical and dental practices maintain compliance within their facilities.

DOCTORS® MANAGEMENT
Leave the business of medicine to us