DUXWARE™
...LEADING THE WAY IN TECHNOLOGY FOR HEALTHCARE PROVIDERS

One Minute HIPAA Compliance

Who Has a Phone?

Prepared by Kenneth E. Rhea, MD, FASHRM

For □ smartphones□ the answer probably is just about everyone including your medical staff. These multi-use devices are capable of receiving and storing protected health information (PHI) received either by data transmission or photography either accidentally or by intent. In one reported incident two nurses were discharged for unauthorized photographing a patient's X Ray and posting on Facebook.[1] Exposure of patient protected health information (PHI) is a serious violation of HIPAA privacy and security regulations.

Recently a medical / surgical practice after loss of a laptop computer containing protected health information (PHI) was investigated for violation of HIPAA privacy and security regulations by the Office for Civil Rights (OCR). The practice entered into a Resolution Agreement (RA) and Corrective Action Plan (CAP) with the OCR.[2] The RA pointed out a number of practice violations including the fact that the practice □ □ did not adequately adopt or implement policies and procedures governing the receipt and removal of portable devices into, out of, and within the facility□ □ and □ □ had no reasonable means of tracking [practice] owned

[1] Fink J. Five Nurses Fired for Facebook Postings, Scrubs Mag. Site: www.scrubsmag.com. http://scrubsmag.com/five-nurses-fired-for-facebook-postings/. June 14, 2010. Accessed December 27, 2014

[2] HHS. Massachusetts provider settles HIPAA case for $1.5 million. OCR. Site: www.hhs.gov. http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/meei-agreement.html, Accessed December 27, 2014.

portable media devices containing its ePHI into and out of its facility, or the movement of these devices within the facility.□ The reference to □ portable devices□ means smartphones, tablets, laptops, etc.[3]

If any smartphones or other portable devices are being used in your medical areas be certain that you have policies in place for their use. Obviously the policies should address the movement of the devices and among other things these policies should require configuration of smartphones holding any protected health information (PHI) to allow remote shutdown and data wiping in case of loss. It has been determined by large studies that about 1/3 of smartphones will at some time be lost and that there is only a 50% chance of having the phone returned.[4] However, even the return of the phone may not assure that data was not breached depending on the phone security in place and whether the data was encrypted.

Having policies is critical as well as procedures to implement the policies and means of assessing whether or not the policies are achieving the desired effect. A generic sample policy can be used as a starting point.

Note: □ sample policy□ link to http://christiansenlaw.net/2012/09/hipaa-mobile-devices-policy-open-source/

DUXWARE™

...LEADING THE WAY IN TECHNOLOGY FOR HEALTHCARE PROVIDERS

www.duxware.com □ 800-248-4298

[3] Ibid

[4] Symantec. Symantec Honey Stick Project. www.symantec.com. http://www.symantec.com/content/en/us/about/presskits/b-symantec-smartphone-honey-stick-project.en-us.pdf. Pub 2012. Accessed November 9, 2013