manatt

Healthcare Law

Safeguarding Patient-Generated Health Information Created or Shared Through Mobile Devices

Aug 03, 2012 | Authors: Robert D.Belfort | Helen R. Pfister | Susan R. Ingargiola

Mobile health technologies are increasingly becoming a valuable tool for improving the quality and efficiency of healthcare. A current example of work in this area involves The Robert Wood Johnson Foundation's Project HealthDesign, which is exploring use of personal health applications to promote better decision-making processes by patients and healthcare providers alike.

Under the most recent phase of the project, researchers are providing patients with smart phones to aggregate and send "observations of daily living" ("ODLs") and other information that can serve as an important indicator of a patient's health to healthcare providers through personal health record applications and other means. However, the use of smart phones and other mobile devices to generate and communicate health information subjects this information to unique security risks for which there are no widely accepted solutions. This is because when healthcare providers handle individually identifiable health information in electronic form, they are subject to the HIPAA Security Rule. But HIPAA regulates providers, not patients. When patients generate health information using applications on their mobile devices, this activity is not governed by the Security Rule. Thus guidance is lacking.

The *Journal of Healthcare Information Management*, in a new article authored by Robert Belfort, Helen Pfister and Susan Ingargiola of Manatt, Phelps & Phillips, LLP, and Deven McGraw of the Center for Democracy & Technology, discusses the types of factors that should be considered when protecting patient-generated health information created on or shared through mobile devices, including:

- The complexity and cost of the security measure.
- The ability of the patient to perform the task.
- The effect the security measure will have on the efficient delivery of clinical care.
- The probability and criticality of potential risks to the information.

The article also recommends specific strategies for securing patient health information on mobile devices and for implementing technical safeguards relating to access restrictions and authentication requirements to ensure general device security.

To read the full article, click here.

Article originally published in JHIM, vol. 26, no. 3 by the Healthcare Information and Management Systems Society. Used with permission.