WILENTZ
—ATTORNEYS AT LAW—
WILENTZ, GOLDMAN & SPITZER, P.A.

Lost Laptops or PDAs? How to Limit Your Exposure Under HIPAA

02/14/13

You have all seen on TV or read in the newspapers of business people losing or having their laptops and personal digital assistants ("PDAs", such as I-Phones) stolen; but do you know as a healthcare professional losing your laptop or PDA might create serious potential liability for you and/or your practice? A medical practice may incur severe civil penalties under the privacy and security regulations adopted pursuant to the federal Health Insurance Portability and Accountability Act of 1996 (the "HIPAA Privacy and Security Rules") if one of its employees loses a laptop or PDA that contains a patient's personal health information ("ePHI") of the ePHI is not properly encrypted. In addition, additional civil or other administrative penalties may result. Moreover, any individual affected by the loss or improper disclosure of their ePHI can also bring a lawsuit against the medical practice and the employee.

No one can guarantee that their laptop or PDA will never be lost or stolen, so medical practices should take reasonable steps to minimize exposure under the HIPAA Privacy and Security Rules and potential costly litigation. Such steps must be based upon a thorough risk analysis of the medical practice and full compliance with the HIPAA Privacy and Security Rules. At a minimum, the practice should do following:

1. Inventory all laptops and PDAs that are used in connection with the medical practice. The inventory should include, at a minimum, the name of the person who has rights to use the device, the exact name of the device, serial number and storage location.
2. If practicable, ensure that no ePHI is ever stored on the device. This may be accomplished by ensuring that any access to ePHI may only be made by connecting to a server and that no ePHI remains on the device.
3. Protect all such devices with appropriate passwords as determined by the medical practice in consultation with the medical practice's IT consultant.
4. Have all such devices properly encrypted. If such a device that contains ePHI is appropriately encrypted in accordance with the HIPAA Privacy and Security Rules and related requirements and guidance, then even if such device is lost or stolen, the ePHI will be deemed to be unusable, unreadable and/or indecipherable. See 74 Fed. Reg. 19006 (Apr. 27, 2009).
5. Properly and timely train all individuals (employees and independent contractors) who have such laptops or PDAs. This training would include, at a minimum, the following: (i) securing the device at all times it is not in use; and (ii) ensuring that the password, encryption and other protections placed on the device are never compromised.
6. Have all such individuals sign a comprehensive certification acknowledging the training and the requirements to abide by the medical practice's policies and procedures in connection with the use and storage of such devices.

To avoid problems and significantly reduce the risks of any possible violation of HIPAA Privacy and Security Rules or other violations of law as well as costly litigation, a medical practice should promptly take at least the above steps. Medical practices are strongly urged to consult with competent legal counsel to guide them through the complexities of the HIPAA Privacy and Security Rules as well as other applicable privacy laws.

Attorney

- Michael F. Schaff

Practice

- Health Law