Lost Thumb Drive Results in a $150,000 Penalty for Small Dermatology Practice

By: Lyndsey Barnett on December 27, 2013 on graydon.law

By: Lyndsey Barnett

This week the Adult & Pediatric Dermatology, P.C. practice agreed to settle a HIPAA violation with HHS. The settlement included the small dermatology practice paying $150,000 payment to HHS, agreeing to perform a comprehensive risk analysis and agreeing to put a risk management plan in place to address and mitigate security risks and vulnerabilities.

This settlement was a result of a notification to HHS by the practice after one of its employees had an unencrypted thumb drive stolen out of the employee's car. The thumb drive contained electronic PHI of approximately 2,200 patients. In accordance with the breach notification rules, the practice gave timely notification to both the impacted patients and to HHS. A month later HHS opened an investigation against the practice. HHS's investigation found that the practice did not conduct an accurate and thorough analysis of the potential risks and vulnerabilities to the confidentiality of electronic PHI until almost a year after the breach occurred. The investigations also found that the practice was in violation of the requirement to have written policies and procedures regarding breach notification and to train employees on such policies and procedures. Finally, the investigation also found that the practice had not reasonably safeguarded the unencrypted thumb drive containing electronic PHI.

There are several lessons to take away from this HHS settlement. First, if you are a covered entity (i.e, a group health plan, health care provider or health care clearinghouse) or a business associate and you have not yet updated your HIPAA policies and procedures for the final HIPAA regulations, you should do so as soon as possible. Second, if you have a breach of PHI, you must make sure that you not only timely report it to impacted individuals, HHS, and the media (if required), but that you take steps to make sure you have not only mitigated the damage done by this breach but to also ensure that it doesn't happen again. Whenever there is a breach or HIPAA violation relating to electronic PHI, it is a good idea to perform a risk analysis to determine where the breakdown happened and what you need to do to increase the protections around PHI. Finally, if you haven't already done so, adopt a policy prohibiting PHI from being saved to thumb drives or requiring that all information

placed on thumb drives be encrypted. Thumb drives are too easy to misplace and this settlement is not the first resolution with HHS that has involved a stiff penalty for the loss of a thumb drive . . . and it likely won't be the last.