The $150,000 PHI Flash Drive

Imagine this, your health care employee loses a flash drive containing

protected health information. You immediately inform the affected patients and the media as required under the breach notification rules of HIPAA and HITECH. You're in the clear, right? Perhaps not, as one health care provider recently learned to the tune of $150,000. **The $150,000 Flash Drive** In October 2011, an employee of Massachusetts based Adult & Pediatric Dermatology, P.C. had their car broken into and one of the items stolen was an unencrypted thumb drive that contained limited medical records of 2,200 patients. Even though there was no evidence that the patient information had been accessed or used by the thief, the practice determined that a breach had occurred and appropriately notified the affected patients and the media. Unfortunately for the practice, the Department of Health and Human Services (HHS) concluded that these actions alone did not fulfill the practice's HIPAA obligations. Specifically, HHS determined the practice had insufficient procedures in place to document its analysis and attempts to mitigate known risks. Further, HHS found that the practice had insufficient workforce training on HIPAA compliance (read more here). This marks the first time a HIPAA enforcement action has been brought for the failure to have sufficient policies, procedures, and training in place. HHS's enforcement director, Leon Rodriguez, indicated that he expects health care providers to be more proactive in preventing risks; stating that being proactive "is what a good risk management process is all about – identifying and mitigating the risk before a bad thing happens." **How to Protect Your Practice** First, if your practice uses portable storage devices or thumb drives that contain PHI, you must make sure they are sufficiently encrypted so that PHI remains secured even if they are lost or stolen. Second, you need to have written documents demonstrating that you have analyzed and mitigated the known risks facing your PHI and that you are routinely training your employees regarding how to respond if a breach occurs. If you need assistance, contact one of Seigfreid Bingham's health care attorneys. We can assist you in conducting and documenting your risk analysis as well as training your employees on HIPAA compliance requirements. Remember, up front compliance costs will almost always be less expensive than paying to fix a breach. Photo: Thinkstock/ISerg