Provider Alert: HIPAA Compliance and Another Costly Missing Laptop

Just before Thanksgiving, Lahey Clinic Hospital, Inc., the well-known Massachusetts teaching hospital and non-profit, signed a settlement agreement with the Department of Health and Human Services, Office of Civil Rights concerning potential violations of the HIPAA privacy rule. As a part of the settlement, Lahey agreed to pay $850,000 and enter into a Corrective Action Plan (CAP) likely to last at least 2 years.

The matter stems from a missing laptop computer used in conjunction with a CT Scanner. The laptop, which contained unencrypted protected health information for 599 individuals went missing in 2011. As a part of its subsequent investigation, the government determined that:

- Lahey failed to conduct an accurate and thorough analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its ePHI as part of its security management process. See 45 C.F.R. §164.308(a)(1)(ii)(A)
- Lahey failed to implement reasonable and appropriate physical safeguards for a workstation that accesses ePHI to restrict access to authorized users. See 45 C.F.R. § 164.310(c).
- With respect to the workstation, Lahey failed to implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of its facility, and the movement of these items within its facility. See 45 C.F.R. § 164.310(d)(1).
- Lahey failed to assign a unique user name for identifying and tracking user identity with respect to the aforementioned workstation. See 45 C.F.R. § 164.312(a)(2)(i).
- Lahey did not implement a mechanism to record and examine activity on the workstation at issue in this breach. See 45 C.F.R. § 164.312(b).
- Lahey impermissibly disclosed the ePHI of 599 individuals for a purpose not permitted by the Privacy Rule. See 45 C.F.R. § 164.502(a).

Pursuant to the Corrective Action Plan, Lahey has to undertake a significant number of corrective measures under close supervision of the Government, at the risk of losing the protection of the settlement, and facing new civil monetary penalties for the 2011 violations.

Given the four year investigation, the compliance costs related to the CAP, as well as the settlement amount, Lahey's financial consequences associated with the lost or stolen laptop likely easily top $1 million. The matter should be a reminder to providers not to overlook the protection of PHI in laboratory and diagnostic imaging equipment, and any other less than obvious place where it may be stored.

A copy of the Lahey settlement and corrective action plan is attached.

For more information, contact Sulloway & Hollis Health Care Group Attorney, Bob Best at 603-223-2812 or by e-mail, RBest@Sulloway.com.