MINTZ

Update on Patient Information Breaches

October 13, 2011 | Blog | By **Cynthia J. Larose**

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

RELATED INDUSTRIES

Written by Dianne Bourque

Nemours Children's Health System has reported the loss of three, **unencrypted** computer backup takes containing patient billing and employee payroll data. The tapes had been stored in a locked cabinet, and were reported missing on September 8th. It is believed that they may have been removed in early August during a facility remodeling project. In an unrelated story, a U.S. District Court judge in Pennsylvania remanded to state court a class action lawsuit stemming from a separate breach of pediatric patient data. In remanding the case, the court emphasized that there is no private right of action under HIPAA.

The Nemours Breach

The information on the Nemours tapes related to approximately 1.6 million patients, patient guarantors, employees, and vendors of Nemours facilities in Delaware, Pennsylvania, New Jersey and Florida. The back up tapes held name, address, date of birth, social security number, insurance information, medical treatment information and bank account information. Affected individuals have been notified and offered one year of identity theft protection and credit monitoring. The press release relating to the breach is here.

The Pennsylvania Decision

If any of the affected Pennsylvania patients intend to sue over the Nemours breach, they should take note of a recent decision out of the U.S. District Court for the Eastern District of Pennsylvania, affirming that there is no private right of action under HIPAA. The Pennsylvania case involved the loss of an unencrypted thumb drive by Keystone Mercy Health Plan. The device contained the personal and medical information of more than 280,000 children.

The plaintiffs originally filed in state court, but insurers for the defendants attempted to remove the case to federal court for an interpretation of HIPAA and the administrative, physical and technical security measures required for compliance. In remanding the case to state court, U.S. District Judge Anita Brody said, "If I were to find jurisdiction and allow this case to proceed in federal court, I would federalize an entire category of state tort claims when Congress has not indicated any intent to do so."

Authors

Cynthia J. Larose, Member / Co-chair, Privacy & Cybersecurity Practice

Cynthia J. Larose is Chair of the firm's Privacy & Cybersecurity Practice, a Certified Information Privacy Professional-US (CIPP-US), and a Certified Information Privacy Professional-Europe (CIPP-E). She works with clients in various industries to develop comprehensive information security programs on the front end, and provides timely counsel when it becomes necessary to respond to a data breach.