LASHLY & BAER, P.C.
ATTORNEYS AT LAW

MISSOURI
714 Locust Street
St. Louis, MO 63101-1699
TEL: 314 621.2939
FAX: 314 621.6844
www.lashlybaer.com

ILLINOIS
20 East Main Street
Belleville, IL 62220-1602
TEL: 618 233.5587
By Appointment Only

Photocopiers – The New Hotspot for HIPAA Risks

By: Stuart J. Vogelsmeier, J.D.
and Tricia J. Mueller, J.D.

Providers: Do you know what information resides on your photocopiers? That question has become one of the most talked about compliance issues related to Protected Health Information under the Health Insurance Portability and Accountability Act ("HIPAA") in the past two months. On August 14, 2013, the Department of Health and Human Services ("HHS") announced that Affinity Health Plan ("Affinity") agreed to settle for $1,215,780 the potential violations of the HIPAA Privacy and Security Rules, resulting from electronic Protected Health Information ("EPHI") that was left on the hard drives of leased photocopiers after the lease term ended.

Affinity, which is a managed care plan in New York, returned photocopiers to its leasing agent at the end of the lease term. Those photocopiers were ultimately sold to another entity (rumored to be CBS Evening News). The entity which purchased the photocopiers notified Affinity that EPHI resided on the hard drives of the photocopiers. Affinity then self-reported the data breach to HHS. The HHS investigation determined that Affinity had impermissibly disclosed EPHI of up to 344,759 individuals when it failed to properly erase photocopier hard drives prior to returning the photocopiers to the leasing company at the end of the lease term. HHS also determined that Affinity failed to assess and identify the potential security risks and vulnerabilities of EPHI stored in the photocopier hard drives, and failed to implement its policies for the disposal of EPHI with respect to the photocopier hard drives.

The Resolution Agreement between HHS and Affinity also required Affinity to take certain "corrective actions":

- Retrieve all photocopier hard drives in the photocopiers previously leased by Affinity that remained in the possession of the leasing company, and safeguard all EPHI contained in the hard drives. If Affinity could not retrieve those hard drives, Affinity was required to provide HHS with documentations explaining its "best efforts" to obtain the hard drives.
- Conduct a comprehensive risk analysis of EPHI vulnerabilities and security risks that incorporates all electronic equipment and systems controlled, owned or leased by Affinity.
- Develop a plan to address and mitigate any security risks and vulnerabilities found in the analysis, and revise all relevant policies and procedure.

The Affinity settlement should raise red flags for all providers. Providers shall consider the following compliance questions:

- Is PHI stored on the hard drives of your photocopies and other electronic devices, such as computers, cell phones, and medical equipment with embedded software?
- Does your organization have a policy safeguarding PHI stored on hard drives?
- Does your organization have a procedure in place to delete the PHI from hard drives upon return, sale, or other disposal of electronic devices such as photocopiers?
- Have you asked your photocopier vendor to provide a technical protocol for deleting PHI from hard drives?
- If the photocopier vendor will actually be involved in deleting the PHI from the hard drives, do you have a written agreement which delineates each party's responsibilities?
- If the photocopier vendor actually takes the photocopier off your premises before removing the PHI, do you have a Business Associate Agreement in place with the vendor, and have you required the vendor to provide a written certification of the completion of this activity?

++

Stuart Vogelsmeier is a partner with Lashly & Baer, P.C. Mr. Vogelsmeier regularly counsels health care providers on issues such as Stark Law and Anti-Kickback Law compliance, corporate structure, employment agreements, joint ventures, adding ancillary services to practices, and asset protection. He can be contacted at (314) 436-8349 or at sjvogels@lashlybaer.com. Tricia J. Mueller also practices in the Lashly & Baer, P.C. Health Care Group. Ms. Mueller advises health care providers on compliance and regulatory issues such as HIPAA, EMTALA, the Stark Law, the Anti-Kickback Law, and fraud and abuse prevention. She can be contacted at (314) 436-8333 or at tmueller@lashlybaer.com. The firm's website is www.lashlybaer.com.