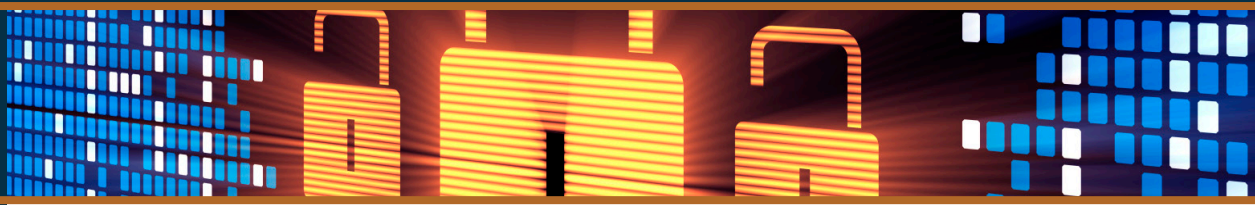
SHIPMAN & GOODWIN® LLP
COUNSELORS AT LAW

HEALTH LAW

August 26, 2013



Health Law Practice Group:

Joan W. Feldman
(860) 251-5104
jfeldman@goodwin.com

David M. Mack
(860) 251-5058
dmack@goodwin.com

Vincenzo Carannante
(860) 251-5096
vcarannante@goodwin.com

William J. Roberts
(860) 251-5051
wroberts@goodwin.com

Alex J. Hwang
(860) 251-5334
ahwang@goodwin.com

www.shipmangoodwin.com

Recent OCR Enforcement Action Demonstrates the Importance of a Thorough Risk Analysis

The United States Department of Health and Human Services Office for Civil Rights ("OCR") recently announced the imposition of monetary penalties and corrective actions against a New York managed care company after the managed care company reported to OCR that patient health information was retained on a leased photocopy machine returned to the leasing company. This enforcement action serves as a stark reminder of the importance of managing equipment and devices that contain protected health information ("PHI").

The Enforcement Action

On April 15, 2010, Affinity Health Plan notified OCR of a breach of the unsecured PHI of nearly 350,000 individuals. Affinity learned of the breach after a representative of the CBS Evening News informed Affinity that it had purchased a copier previously leased by Affinity and that the copier contained confidential health information on its hard drive.

Upon notification, OCR investigated the incident and its investigation indicated that Affinity impermissibly disclosed PHI when it returned multiple copiers to its leasing agents without erasing the data from each copier's hard drive. Affinity settled the potential violations by agreeing to a $1,214,780 payment and a corrective action plan requiring Affinity to, among other things, retrieve other hard drives on copiers previously leased by it.[1]

Implications

In its settlement, OCR emphasized Affinity's failure to consider photocopier hard drives in its risk analysis - the process by which HIPAA covered entities determine where PHI is used and maintained and how to best mitigate risks to such PHI. OCR also required Affinity to conduct a "comprehensive risk analysis" which suggests that OCR believed Affinity's prior risk analysis to be inadequate.

OCR's focus on Affinity's risk analysis, and the significant breach which resulted from Affinity's failure to erase data maintained on the leased photocopiers, highlight the

1 A copy of the settlement agreement is available here: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/affinity_agreement.pdf.

One Constitution Plaza
Hartford, CT 06103-1919
860-251-5000

300 Atlantic Street
Stamford, CT 06901-3522
203-324-8100

1133 Connecticut Avenue NW
Washington, DC 20036-4305
202-469-7750

289 Greenwich Avenue
Greenwich, CT 06830-6595
203-869-5600

12 Porter Street
Lakeville, CT 06039-1809
860-435-2539

www.shipmangoodwin.com

importance of conducting a thorough risk analysis. The risk analysis should carefully consider and address all ways in which a covered entity and its employees use, maintain and disclose PHI. Keep in mind that PHI may be contained in unlikely places. When conducting a risk analysis, we suggest the following:

- Consider carefully where PHI you collect or maintain is stored or used, including computer systems, mobile devices, copiers, medical equipment, facsimile machines, and paper storage. Pay particular attention to cell phones, USB drives, and cloud storage applications.
- If your organization uses any telehealth devices or applications, note that such devices may contain PHI even when the device is not in your possession. This is particularly true for certain remote monitoring devices. In addition, many medical devices and equipment maintain PHI.
- Consider obtaining an independent analysis of your PHI use and storage. It is often beneficial to have a fresh set of eyes.
- Prepare an inventory of all the devices your business or employees possess that maintain PHI.
- Adopt policies to ensure that upon disposal or transfer of a device to a third party all PHI maintained on that device is erased in accordance with industry standards.
- Review and utilize resources made available by government regulators. The National Institute of Standards and Technology publishes a wide range of resources for securing data, including encryption, data transmission, data storage and securing mobile devices. Such publications are available at http://csrc.nist.gov/publications/PubsSPs.html. Of particular note in light of *Affinity* is *Computer Security: Guidelines for Media Sanitization* available at http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800_88_r1_draft.pdf. In addition, covered entities concerned about their photocopiers are encouraged to consider *Copier Data Security: A Guide for Businesses published by the Federal Trade Commission* and available at http://business.ftc.gov/documents/bus43-copier-data-security.

Questions?

Shipman & Goodwin offers a team of experienced lawyers who have been counseling clients on health care data privacy issues for many years. We are able to provide practical, cost effective solutions to the problems our clients face. If you have any questions about this Alert or data privacy and security in general, please contact any member of our Health Law Practice Group listed on the first page of this alert.

SHIPMAN & GOODWIN® LLP