Healthcare Law Alert – Stolen Backup Media Leads to $750,000 Settlement

Cancer Care Group, Inc. (the Group), a physician practice comprised of approximately thirteen radiologists, recently settled with the Department of Health and Human Services' Office of Civil Rights (OCR) for $750,000 to resolve potential violations of HIPAA's Privacy and Security Rules. In July 2012, a laptop bag containing a computer and an unencrypted backup media device was stolen from an employee's car. Unfortunately, the stolen backup device held unsecured electronic protected health information (ePHI) including the names, addresses, dates of birth, Social Security Numbers, insurance information and clinical information of approximately 55,000 current and former patients. Had the stolen media device been encrypted using certain approved technologies, breach notification under HIPAA would not have been required following the theft – the Group would have be able to take advantage of the so-called encryption safe harbor.

The Group reported the breach to OCR in August 2012 and reached a settlement with OCR three years later. The settlement includes the fine of $750,000 and a resolution agreement which includes a corrective action plan, requiring in part that the Group report certain HIPAA compliance activities to OCR over the next few years.

OCR's investigation of the breach also uncovered potential serious non-compliance with HIPAA by the Group that was unrelated to the theft, including i) failure to conduct an enterprise-wide security risk analysis; ii) failure to implement policies and procedures governing the movement of hardware and electronic media containing ePHI into, out of and within the Group's facility; and iii) failure to safeguard unencrypted backup media.

No organization wants to experience a breach of its patients' health information. It is safe to assume, however, that for most organizations, breaches are inevitable despite the best of intentions. What makes matters worse, in OCR's view, is when a breach occurs and the organization has failed to understand its risks (through a risk analysis) and/or failed to implement written policies to guard against such risks.

The Security Rule requires, among other things, that an organization determine via a risk analysis whether encryption of portable devices containing ePHI is a reasonable and appropriate measure to take. In the case above, OCR noted that if the Group had performed a risk assessment, it could have identified the removal of unencrypted portable media as an area of significant risk to ePHI, and could have addressed the concern prior to the breach, for example, through encryption.

In sum, HIPAA Covered Entities and their business associates must conduct and document a risk analysis in accordance with HIPAA, and not simply as a one-time event. Following an initial risk assessment, organizations should repeat the risk assessment periodically, including but not limited to any time a material change to their information technology system occurs. In addition, Covered Entities must deploy and update their HIPAA policies and procedures as needed. If vulnerabilities are

discovered through the risk assessment or by other means, they must fix the issues and amend their policies accordingly. Should there be a breach, OCR will look to see if these policies and procedures existed/were followed and, if not, the agency is likely to impose harsher penalties than would otherwise be the case.

Finally, if an organization is still unsure whether encryption is a worthwhile investment, we suggest taking a look at OCR's list of breaches, particularly those resulting from stolen devices containing unsecured ePHI for the answer, noted in the below link:

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Visit our Healthcare Practice Area to learn more about the legal services we can provide in these areas. If you have any questions or would like more information on the issues discussed in this communication, please contact any member of our Healthcare Practice Area.