NCADA NORTH CAROLINA ASSOCIATION OF DEFENSE ATTORNEYS

The Resource

July 2016 Feature Article

High Stakes Privacy Breaches – The First Business Associate Settlement Brings HIPAA Compliance Into Sharper Focus for Law Firms

Beth Stanfield, Lincoln Derr, PLLC

Since 2013, when the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) issued its Final Rule implementing revisions to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the potential for business associates to be sanctioned for privacy breaches has been a concern to law firms that regularly handle protected health information (PHI). A recent settlement involving a business associate brings that concern into sharper focus.

But first, a brief HIPAA refresher . . .

The 2013 revisions to HIPAA, which were mandated by the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act), extended the privacy and security requirements originally focused on healthcare providers (or "covered entities") to business associates. In recognition of the fact that most healthcare providers rely on outside providers to carry out various healthcare functions, the definition of "business associate" encompasses a wide variety of outside providers, such as third party administrators, CPAs, transcriptionists, and attorneys. In fact, the website for HHS provides several examples of groups that would be considered business associates under the HITECH Act, including "[a]n attorney whose legal services to a health plan involve access to protected health information."

Given the high stakes associated with a potential privacy breach, law firms have been working to solidify their security measures and protocols both internally and with outside contractors to comply with all HIPAA and HITECH Act requirements. However, the recent business associate settlement published on the website for HHS provides greater insight into the potential for a HIPAA violation and the degree of security measures necessary to remain in compliance.

The subject of the settlement was Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS), a non-profit organization providing management services to six nursing homes. In February 2014, OCR was notified by each of the nursing homes regarding a breach of unsecured electronic PHI (ePHI). The potential breach arose from a stolen iPhone, which contained ePHI of nursing home residents. Specifically, the phone contained social security numbers, information regarding diagnosis and treatment, medical procedures, names of family members and legal guardians, and residents' medication information.

After investigating the incident, OCR determined that CHCS (1) failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and

availability of ePHI held by CHCS; and (2) failed to implement appropriate security measures sufficient to reduce the risks and vulnerabilities to a reasonable and appropriate level. The investigation revealed that the phone, which was issued by CHCS to an employee, was not encrypted or password protected. In addition, CHCS did not have any policies addressing removal of devices with PHI or what to do in the event of a security incident. Finally, OCR determined CHCS did not have a "risk analysis" or "risk management plan."

As a part of the settlement, CHCS agreed to pay $650,000.00 and entered into an "Agreement and Corrective Action Plan" on June 24, 2016.

The corrective action measures outlined in the Agreement are instructive for business associates. For example, CHCS was required to promulgate numerous policies addressing the following items:

- encryption of ePHI;
- password management;
- security incident response;
- mobile device controls;
- information system review;
- security reminders;
- log-in monitoring;
- a data backup plan;
- a disaster recovery plan;
- an emergency mode operation plan;
- testing and revising of contingency plans;
- applications and data criticality analysis;
- automatic log off;
- audit controls; and
- integrity controls.

The Agreement further required CHCS to review its policies at least annually (if not more often) and distribute them to its workforce. CHCS was also required to obtain "signed written or electronic initial compliance certification from all members of [its] workforce" and provide security training.

In addition to the financial and administrative implications of OCR's investigation, perhaps of even greater concern to business associates is the negative exposure associated with such a well-publicized settlement arising from a fairly common occurrence – theft of an iPhone. While the Agreement and Corrective Action Plan disclaims any admission of liability on the part of CHCS, the Agreement is fully accessible to the public and available here.

About the Author

Beth Stanfield is a skilled, committed litigator handling high-stakes civil litigation in state and federal courts. Ms. Stanfield's experience spans a wide variety of fields, including medical malpractice defense, business and commercial litigation, debtor-creditor matters, employment disputes, derivative actions and shareholder disputes, breach of contract claims, trademark and copyright infringement litigation, municipal liability and police use of force claims, personal injury/wrongful death claims, as well as premises, toxic tort, and products liability litigation. Ms. Stanfield has substantial experience as a trial lawyer, defending clients in multi-week and even multi-month trials with significant exposure.