

HHS Scores Record Settlement Against Advocate Health in HIPAA Enforcement Case

With a dozen acute-care hospitals and more than 250 treatment locations to its name,

Advocate Health Care is the largest healthcare system in Illinois. It recently earned another superlative, though this is a dubious distinction: owing the Health and Human Services (HHS) the [largest Health Insurance Portability and Accountability Act \(HIPAA\) settlement ever awarded](#)—\$5.55 million.

According to the HHS Office for Civil Rights (OCR), the hefty figure reflects how long the HIPAA violations had been occurring and the sheer number of individuals affected.

Unencrypted data falls into the wrong hands; consumers placed at risk

Patients expect their [protected health information \(PHI\)](#) to be just that—protected. But since 2013, patients with Advocate Health Care have not been guaranteed that protection, unbeknownst to them. The health system itself reported the three breaches to HHS; following three breach notifications in the space of four months, HHS opened an investigation into Advocate's data security practices.

The first—and most significant—breach was reported in August of 2013, and stemmed from the theft of four Advocate laptops containing nearly four million patient records. The data was unencrypted. HHS reports that this was the second-largest records breach since the OCR began posting major violations on its public “wall of shame.” The health system was the subject of multiple lawsuits due to this breach; the first two class action suits would be dismissed by July of 2014.

Two more breaches occurred after that, one to the network of a business associate, and one to Advocate's ePHI system. Approximately 2,000 individuals were affected in each of those events.

Advocate released a statement assuring the public that its top priority is protecting patient privacy and confidentiality and stating that it intends to fully cooperate with the government to enhance its data security.

“As all industries deal with the ever-evolving digital landscape and the impact it has on security, we've enhanced our data encryption measures to prevent this type of incident from reoccurring,” Advocate Health Care said. “While there continues to be no indication that the information was misused, we deeply regret any inconvenience this incident has caused our patients.”

Office for Civil Rights sending a “strong message” to health systems

OCR determined that Advocate had not appropriately evaluated risks to its IT systems and further, that it failed to



establish reasonable practices to anticipate and protect against dangers.

OCR Director Jocelyn Samuels had this to say about the record-setting figure: “We hope this settlement sends a strong message to covered entities that they must engage in a comprehensive risk analysis and risk management to ensure that individuals’ ePHI [electronic patient health information] is secure. This includes implementing physical, technical, and administrative security measures sufficient to reduce the risks to ePHI in all physical locations and on all portable devices to a reasonable and appropriate level.”

The terms of the settlement demand that Advocate conduct a thorough risk assessment and develop strategies approved by HHS for securing IT systems that deal with PHI.

HHS making the mark in other HIPAA-enforcement cases

Advocate is not alone in feeling the heat from HHS HIPAA-enforcement: last month the HHS was successful against the University of Mississippi Medical Center and Oregon Health and Science University with \$2.75 million and \$2.7 million settlements, respectively.

It’s likely that the OCR’s message is being heard—resounding!

For more information/questions regarding any legal matters, please email info@nelsonhardiman.com or call 310.203.2800.