
THE WORST HIPAA-RELATED INCIDENTS OF 2016

Raleigh Orthopaedic Clinic, P.A. of North Carolina – $750,000

Raleigh Orthopaedic Clinic, P.A. of North Carolina (Raleigh Orthopaedic), a multi-physician orthopaedic practice serving Wake County, N.C., agreed to pay a $750,000 settlement following investigation of a 2013 breach involving 17,300 patients. Raleigh Orthopaedic transferred X-ray films and associated PHI to a third-party who was supposed to digitize the images and harvest the silver from the X-rays. However, Raleigh Orthopaedic did not have a signed business associate agreement on file prior to the transfer.

Besides the settlement, the organization must also revise business associate policies and procedures as part of a two-year corrective action plan.

Sources: U.S. Department of Health and Human Services (HHS)

North Memorial Health Care – $1.55 Million

North Memorial Health Care (North Memorial), a not-for-profit health care system in Robbinsdale, Minn., was ordered to pay a $1.55 million settlement following two significant violations. In 2011, North Memorial reported the theft of an unencrypted laptop, containing ePHI of nearly 9,500 individuals, from the vehicle of a business associate's employee. OCR's investigation found that North Memorial gave their business associate, Accretive Health, Inc., access to the ePHI of 289,904 patients without having a binding business associate agreement on file. North Memorial also failed to complete a thorough risk assessment to identify vulnerabilities in the handling of ePHI.

In addition to the settlement, North Memorial must implement an organization-wide risk analysis and risk management plan as well as provide further staff training.

Source: HHS

St. Joseph Health – $2.14 Million

St. Joseph Health (St. Joseph), a nonprofit integrated Catholic health care delivery system serving California, Texas, and New Mexico, was ordered to pay $2.14 million due to unauthorized exposure of patients' ePHI. From February 2011 to February 2012, patient data was publicly accessible via the Internet, exposing the names, lab results, and demographic information of 31,800 patients. A file-sharing application included as a default setting of the organization's server permitted the disclosure of the data. St. Joseph failed to modify the default settings when the server was implemented.

In addition to the settlement, St. Joseph agreed to a corrective action plan that includes conducting an enterprise-wide risk analysis and staff training.

Sources: HHS

New York Presbyterian Hospital – $2.2 Million

New York Presbyterian Hospital (NYP), a nonprofit university hospital in New York City, was ordered to pay a $2.2 million settlement after exposing two patients' PHI during filming of the ABC television series, NY Med, in 2013. OCR's investigation found that NYP allowed the film crew to record the death of one patient as well as another in considerable distress despite requests from at least one medical professional for filming to cease. The patients' PHI was disclosed to ABC film crews and staff during this time without obtaining written consent from the patients.

For its part, NYP must also implement a corrective action plan and undergo two years of monitoring by the OCR.

Source: HHS

Oregon Health & Science University – $2.7 Million

Oregon Health & Science University (OHSU), which includes a public university and two hospitals in Portland, Ore., agreed to a $2.7 million settlement following multiple violations that led to the exposure of thousands of patients' ePHI. In 2013, OHSU reported two separate incidents including theft of two unsecured laptops and an unencrypted thumb drive. Upon investigation, OCR discovered that a cloud-based server containing ePHI of 3,000 individuals was also being used without a valid business associate agreement.

In addition to the monetary settlement, OHSU agreed to adopt a comprehensive three-year corrective action plan.

Source: HHS

University of Mississippi Medical Center – $2.75 Million

University of Mississippi Medical Center (UMMC), an academic medical center in Jackson, Miss., was ordered to pay a $2.75 million settlement due to multiple HIPAA violations affecting approximately 10,000 patients. In March 2013, UMMC's privacy officer reported that a laptop was missing from the organization's medical intensive care unit (MICU). Internal investigations revealed that the laptop was likely stolen by a MICU visitor. While the laptop was password-protected, the OCR determined that use of a generic username and password would grant users access to a directory containing ePHI.

Besides the settlement, UMMC must adopt a corrective action plan to ensure future compliance.

Source: HHS

Feinstein Institute for Medical Research – $3.9 Million

Feinstein Institute for Medical Research (FIMR), a nonprofit biomedical research institute in Manhasset, N.Y., and a subsidiary of the health system Northwell Health, Inc., agreed to pay $3.9 million related to a 2012 breach. The ePHI of 13,000 patients and research study participants was compromised when an unsecured laptop was stolen from an employee's vehicle. The laptop stored data such as social security numbers, diagnoses, and laboratory results.

FIMR failed to properly implement policies and procedures related to the transport of devices and hardware containing ePHI. The organization must also adopt a comprehensive three-year corrective action plan.

Source: HHS

Advocate Health Care Network – $5.55 Million

Advocate Health Care Network, the largest health system in Illinois, agreed to pay a $5.55 million settlement following three separate 2013 breaches involving one of its subsidiaries, Advocate Medical Group. Altogether, the ePHI of approximately 4 million individuals was compromised when four desktop computers were stolen from an office building and an unencrypted laptop was taken from an employee's vehicle. The third breach occurred when a third-party accessed the network of one of Advocate's business associates.

This represents the largest settlement for a single entity to-date. Advocate also agreed to adopt a corrective action plan.

Source: HHS