U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

2018 OCR HIPAA Summary: Settlements and Judgments

January 2018

In January 2018, OCR settled for $100,000 with Filefax, Inc., a medical records maintenance, storage, and delivery services provider. OCR's investigation found that Filefax impermissibly disclosed protected health information (PHI) by leaving the PHI in an unlocked truck in the Filefax parking lot, or by granting permission to an unauthorized person to remove the PHI from Filefax, and leaving the PHI unsecured outside the Filefax facility.

In January 2018, OCR also settled for $3.5 million with Fresenius Medical Care North America (FMCNA), a provider of products and services for people with chronic kidney failure. FMCNA filed five breach reports for separate incidents occurring between February 23, 2012 and July 18, 2012, implicating the electronic protected health information (ePHI) of five FMCNA owned covered entities. OCR's investigation revealed that FMCNA failed to conduct an accurate and thorough risk analysis of potential risks and vulnerabilities to the confidentiality, integrity, and availability of all of its ePHI. Additional potential violations included failure to implement policies and procedures and failure to implement a mechanism to encrypt and decrypt ePHI, when it was reasonable and appropriate to do so under the circumstances.

June 2018

In June 2018, an HHS Administrative Law Judge ruled in favor of OCR and required The University of Texas MD Anderson Cancer Center (MD Anderson), a Texas cancer center, to pay $4.3 million in civil money penalties for HIPAA violations. OCR investigated MD Anderson following three separate data breach reports in 2012 and 2013 involving the theft of an unencrypted laptop from the residence of an MD Anderson employee and the loss of two unencrypted universal serial bus (USB) thumb drives containing the unencrypted ePHI of over 33,500 individuals. OCR's investigation found that MD Anderson had written encryption policies going back to 2006 and that MD Anderson's own risk analyses had found that the lack of device-level encryption posed a high risk to the security of ePHI. Despite the encryption policies and high risk findings, MD Anderson did not begin to adopt an enterprise-wide solution to encrypt ePHI until 2011, and even then it failed to encrypt its inventory of electronic devices containing ePHI between March 24, 2011 and January 25, 2013. This matter is under appeal with the HHS Departmental Appeals Board.

September 2018

In September 2018, OCR announced that it has reached separate settlements totaling $999,000, with Boston Medical Center (BMC), Brigham and Women's Hospital (BWH), and Massachusetts General Hospital (MGH) for compromising the privacy of patients' PHI by

inviting film crews on premises to film an ABC television network documentary series, without first obtaining authorization from patients.

In September 2018, OCR also settled with Advanced Care Hospitalists (ACH), a contractor physician group, for $500,000. ACH filed a breach report confirming that ACH patient information was viewable on a medical billing services' website. OCR's investigation revealed that ACH never had a business associate agreement with the individual providing medical billing services to ACH, and failed to adopt any policy requiring business associate agreements until April 2014. Although ACH had been in operation since 2005, it had not conducted a risk analysis or implemented security measures or any other written HIPAA policies or procedures before 2014.

October 2018

In October 2018, OCR settled with Allergy Associates, a health care practice that specializes in treating individuals with allergies, for $125,000. In February 2015, a patient of Allergy Associates contacted a local television station to speak about a dispute that had occurred between the patient and an Allergy Associates' doctor. OCR's investigation found that the reporter subsequently contacted the doctor for comment and the doctor impermissibly disclosed the patient's PHI to the reporter.

In October 2018, Anthem, Inc. also paid $16 million to OCR and agreed to take substantial corrective action to settle potential violations of the HIPAA Rules after a series of cyberattacks led to the largest U.S. health data breach in history. Anthem filed a breach report after discovering cyber-attackers had gained access to their IT system via an undetected continuous and targeted cyberattack for the apparent purpose of extracting data, otherwise known as an advanced persistent threat attack. After filing their breach report, Anthem discovered cyber-attackers had infiltrated their system through spear phishing emails sent to an Anthem subsidiary after at least one employee responded to the malicious email and opened the door to further attacks. OCR's investigation revealed that between December 2, 2014 and January 27, 2015, the cyber-attackers stole the ePHI of almost 79 million individuals, including names, social security numbers, medical identification numbers, addresses, dates of birth, email addresses, and employment information.

November 2018

In November 2018, Pagosa Springs Medical Center (PSMC), a critical access hospital, paid $111,400 to OCR to resolve potential violations concerning a former PSMC employee that continued to have remote access to PSMC's web-based scheduling calendar, which contained patients' ePHI, after separation of employment. OCR's investigation revealed that PSMC impermissibly disclosed the ePHI of 557 individuals to its former employee and to the web-based scheduling calendar vendor without a business associate agreement in place.

December 2018

In December 2018, Cottage Health agreed to pay $3 million to OCR and to adopt a substantial corrective action plan to settle potential violations of the HIPAA Rules concerning two breach reports of unsecured ePHI affecting over 62,500 individuals. The breaches exposed unsecured ePHI over the internet including patient names, addresses, dates of birth, Social Security numbers, diagnoses, conditions, lab results and other treatment information. OCR's investigation revealed that Cottage Health failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the ePHI; failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level; failed to implement procedures to perform periodic technical and nontechnical evaluations in response to environmental or operational changes affecting the security of ePHI; and failed to obtain a written business associate agreement with a contractor that maintained ePHI on its behalf.

Date	Name	Amount
Jan. 2018	Filefax, Inc (settlement)	$ 100,000
Jan. 2018	Fresenius Medical Care North America (settlement)	$ 3,500,000
June 2018	MD Anderson (judgment)	$ 4,348,000
Aug. 2018	Boston Medical Center (settlement)	$ 100,000
Sep. 2018	Brigham and Women's Hospital (settlement)	$ 384,000
Sep. 2018	Massachusetts General Hospital (settlement)	$ 515,000
Sep. 2018	Advanced Care Hospitalists (settlement)	$ 500,000
Oct. 2018	Allergy Associates of Hartford (settlement)	$ 125,000
Oct. 2018	Anthem, Inc (settlement)	$ 16,000,000
Nov. 2018	Pagosa Springs (settlement)	$ 111,400
Dec. 2018	Cottage Health (settlement)	$ 3,000,000
	Total (settlements and judgment)	$ 28,683,400