

2020's a Bust, but HIPAA Enforcement Is on a Roll!

October 15, 2020 – Dorsey Health Law
by Alissa Smith and Elizabeth Greiter

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) has been actively enforcing HIPAA regulations this year, including a series of seven settlements under OCR's Right of Access Initiative to enforce patients' rights to timely access their medical records at a reasonable cost. This year, OCR has recorded more than \$12.2 million in resolution agreements. This post summarizes OCR's settlements in 2020 to date. The OCR settlements have impacted a wide range of sectors in the health industry from health insurers, to hospital systems, physician clinics, FQHCs, mental health and substance abuse providers, business associates, and nonprofits serving those with AIDS/HIV. Enforcement has been taken against all sizes of entities, including against solo practitioners and very small non-profits. As with nearly all settlements with OCR, it was the initial breach notification that triggered the investigation. However, the settlement ultimately resulted after OCR's investigation discovered widespread non-compliance with HIPAA's privacy and security requirements. The following post provides a summary of these enforcement actions, and begins with an update about Anthem's recent \$39.5M settlement with 43 states and D.C. stemming from its massive data breach in 2014-2015, which resulted in a record \$16 million settlement with OCR in 2018.

Health Insurer Enforcement

Anthem and 43-State Coalition Reach \$39.5 Million Settlement Over Data Breach

On September 30, 2020, state attorneys general in 43 states and Washington D.C. announced that they had reached a \$39.5 million settlement with Anthem Inc., an Indianapolis, IN-based health

Related People

- Alissa Smith

Related Capabilities

- Healthcare & Life Sciences
- Healthcare Transactions & Regulations
- Healthcare Litigation
- Medical Devices



insurer. This settlement stemmed from an investigation by the state attorneys general into the largest health data breach in history, a series of state-sponsored cyberattacks in December 2014 and January 2015 that exposed the ePHI of nearly 79 million individuals. In 2018, Anthem agreed to pay \$16 million to OCR and to take substantial corrective action to settle potential violations of the HIPAA privacy and security rules related to the 2014 data breach. See the HHS press release about the OCR settlement [here](#). Anthem has also paid \$115 million to settle a class action related to the breach, the largest-ever class action settlement related to a data breach.

Premiera Blue Cross Pays \$6.85 Million to Settle Data Breach Affecting Over 10.4 Million People

In March, in the second-largest HIPAA settlement ever, Premiera Blue Cross (PBC), the largest health plan in the Pacific Northwest, agreed to pay \$6.85 to OCR and to implement a corrective action plan to settle potential HIPAA privacy and security rules violations related to a data breach. Using malware installed through a phishing email, cyber-attackers gained access to PBC's system in August 2014 and went undetected until January 2015, resulting in the exposure of over 10.4 million individuals' electronic protected health information (ePHI). OCR's investigation determined that PBC had "systemic noncompliance with the HIPAA Rules including failure to conduct an enterprise-wide risk analysis, and failures to implement risk management, and audit controls." See the HHS press release [here](#).

Hospital and Health System Enforcement

Lifespan Pays \$1.04 Million to Settle Unencrypted Stolen Laptop Breach Affecting Over 20,000 People

In June, Lifespan Health System Affiliated Covered Entity ("Lifespan ACE"), a Rhode Island-based non-profit health system, agreed to pay a \$1.04 million settlement to OCR and to adopt a corrective action plan to settle potential violations of the HIPAA privacy and security rules related to the theft of a hospital employee's unencrypted laptop. The laptop contained the ePHI of more than 20,000 individuals. OCR's investigation determined that there had been systematic noncompliance with the HIPAA Rules, including a failure to encrypt ePHI on laptops, a lack of device and media controls, and a failure to have a business associate agreement in place with the Lifespan Corporation, the parent company and business associate of Lifespan ACE. See the HHS press release [here](#).

Physician and Clinic Enforcement

Solo Practice Pays \$100,000 for Failing to Implement HIPAA Security Rule Requirements

In February, Steven A. Porter, M.D., a Utah gastroenterologist and solo practitioner, agreed to pay \$100,000 to OCR and to adopt a corrective action plan to settle a potential violation of the HIPAA security rule. OCR determined that Dr. Porter's practice had

demonstrated significant noncompliance with the HIPAA rules, specifically, failing to conduct any risk analysis and failing “to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.” See the HHS press release [here](#).

Orthopedic Clinic Pays \$1.5 Million to Settle Systemic Noncompliance with HIPAA Privacy and Security Rules

In July, Georgia-based Athens Orthopedic Clinic PA (“Athens Orthopedic”) agreed to pay \$1.5 million to OCR and to implement a corrective action plan to settle potential violations of the HIPAA privacy and security rules. A hacker used a vendor’s credentials to access Athens Orthopedic’s electronic medical record system and exfiltrated patient health data, then demanded money from Athens Orthopedic in return for the return of the stolen records. Nearly 210,000 individuals were affected by the breach. OCR’s investigation found noncompliance with the HIPAA privacy and security rules, including “failures to conduct a risk analysis, implement risk management and audit controls, maintain HIPAA policies and procedures, secure business associate agreements with multiple business associates, and provide HIPAA Privacy Rule training to workforce members.” See the HHS press release [here](#).



FQHC Pays \$25,000 for Failing to Implement HIPAA Security Rule Requirements

In March, Metropolitan Community Health Services (“Metro”), doing business as Agape Health Services, agreed to pay \$25,000 to OCR and to implement a corrective plan to settle potential violations of the HIPAA security rule. In 2011, Metro reported impermissible disclosure of PHI to an unknown email account, which affected over 1,200 patients. OCR’s investigation found that Metro had failed to conduct any risk analysis, failed to implement any HIPAA security rule policies and procedures, and not provided workforce members with security awareness training until 2016. Metro is a Federally Qualified Health Center that provides medical services in underserved areas in rural North Carolina on a sliding fee scale, which was taken into account in reaching this agreement. See the HHS press release [here](#).

Business Associate Enforcement

CHSPSC Agrees to Pay \$2.3 Million to Settle Data Breach Affecting Over 6 Million People

In March, CHSPSC LLC (“CHSPSC”) agreed to pay \$2.3 million and to adopt a corrective action plan to settle potential violation of the HIPAA privacy and security rules related to a breach affecting more than 6 million people. CHSPSC is based in Tennessee and provides a variety of business associate services, including IT and health information management. In 2014, the Federal Bureau of Investigation (FBI) notified CHSPSC that it had traced a cyber-attack to CHSPSC’s information system. OCR’s subsequent

investigation found “longstanding, systematic noncompliance” with the HIPAA security rule, including “failure to conduct a risk analysis, and failures to implement information system activity review, security incident procedures, or access controls.” See the HHS press release [here](#).

Right of Access Initiative **Enforcement**

In 2019, OCR announced the Right of Access Initiative as an enforcement priority to support individuals’ right to timely access to their health records at a reasonable cost and in the readily producible format of their choice under the HIPAA privacy rule’s right of access provision, 45 CFR §

164.524. The HIPAA Rules generally require covered health care providers to provide medical records within 30 days of the request and providers can only charge a reasonable cost-based fee. This right to patient records extends to parents seeking access to their minor children’s medical records.



To date this year, OCR has completed seven enforcement actions totaling \$396,500 in settlement payments under the Right of Access Initiative, bringing the total number of enforcement settlements under this initiative to nine.

- In June, Housing Works Inc. (Housing Works), a New York City-based non-profit organization providing a range of services to individuals living with and affected by HIV/AIDS, including health care, agreed to pay \$38,000 to OCR and to take corrective actions to settle a potential right of access violation. In complaints filed with OCR in July and August 2019, a patient alleged that he had not received his records in response to a June 2019 request. OCR opened an investigation, found a possible violation, and the patient received his medical records in November 2019.
- In July, All Inclusive Medical Services (AIMS), a California-based multi-specialty family medicine clinic, has agreed to pay \$15,000 to OCR and to adopt a corrective action plan to settle a potential right of access violation. A patient alleged that in January 2018, AIMS had denied her requests to inspect and receive a copy of her records, in an April 2018 complaint filed with OCR. The patient ultimately received her medical records in August 2020.
- In August, Beth Israel Lahey Health Behavioral Services (BILHBS), the largest network of mental health and substance use disorder services in eastern Massachusetts, agreed to pay \$70,000 to OCR and to take corrective actions following a potential right of access violation. A personal representative filed a complaint with OCR in April 2019 alleging that she had requested her father’s medical records in February 2019 and BILHBS had failed to provide them. BILHBS provided the requested medical records in October 2019.
- In August, Patricia King, M.D. (King MD), a small provider of psychiatric services in Virginia, agreed to pay \$3,500 to OCR and to adopt a corrective action plan to settle a potential right of access violation. OCR received a complaint from a patient in October 2018, alleging that King MD failed to respond to her August 2018 request for her

medical records. After OCR provided King MD with technical assistance on right of access requirements, a second complaint, and an OCR investigation that found that the failure to provide the requested medical records was a potential violation, the patient received her medical records in July 2020.

- In August, Wise Psychiatry, PC (Wise Psychiatry) a small provider of psychiatric services in Colorado, agreed to pay \$10,000 to OCR and to take corrective actions to settle a potential right of access violation. A father requested his minor son's medical records in November 2017, and following two complaints to OCR, OCR providing technical assistance to Wise Psychiatry on the HIPAA right of access requirements, and OCR opening an investigation, Wise Psychiatry sent the requested medical records in May 2019.

See HHS's press release about OCR's first five right to access settlements of 2020 [here](#).

- In September, Dignity Health, doing business as St. Joseph's Hospital and Medical Center (SJHMC), agreed to pay \$160,000 and to adopt a corrective action plan to settle a potential right of access violation. SJHMC is based in Arizona and is a large, acute-care hospital with several hospital-based clinics. A mother made several requests for her son's medical records, as his personal representative, beginning in January 2018, but did not receive all of the requested records until December 2019. See the HHS press release [here](#).
- In September, NY Spine Medicine (NY Spine), a private medical practice specializing in neurology and pain management with offices in New York and Florida, agreed to pay \$100,000 and to take corrective actions to settle a potential right of access violation. A patient requested a copy of her medical records in June 2019, and NY Spine provided some records in response, but did not provide the diagnostic films that the patient had specifically requested until October 2020, after OCR had initiated an investigation. See the HHS press release [here](#).

OCR's enforcement of the HIPAA security and privacy rules this year is increasingly aggressive. Per HHS, OCR's enforcement actions are "designed to send a message to the health care industry about the importance and necessity of compliance with the HIPAA Rules." If you have questions about HIPAA compliance, please contact the authors, your regular Dorsey attorney or any attorney in the Dorsey & Whitney health transactions and regulations practice group.