Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance

For Calendar Year 2018

As Required by the Health Information Technology for Economic and Clinical Health (HITECH) Act, Public Law 111-5, Section 13424

Submitted to the
Senate Committee on Health, Education, Labor, and Pensions,
House Committee on Ways and Means, and
House Committee on Energy and Commerce

U.S. Department of Health and Human Services
Office for Civil Rights

Introduction

Section 13424(a) of the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as title XIII of division A and title IV of division B of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5), requires the Secretary of Health and Human Services (the Department) to prepare and submit an annual report to the Senate Committee on Health, Education, Labor, and Pensions and to the House Committee on Ways and Means, and the House Committee on Energy and Commerce (the Committees), regarding compliance with the Privacy and Security Rules promulgated under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Pub. L. 104-191), as well as the privacy, security, and breach notification provisions of the HITECH Act. Thus, for the year for which the report is prepared, the report summarizes the Department's compliance and enforcement activities with respect to the HIPAA Privacy, Security, and Breach Notification Rules at 45 CFR Parts 160 and 164 (collectively, the HIPAA Rules or the Rules). Section 13424(a)(2) of the HITECH Act requires that each report be made available to the public on the website of the Department.

Section 13424(a)(1) of the HITECH Act requires that the report include, with respect to complaints received and compliance reviews begun during the reported year(s):

- the number of complaints received by HHS from the public;
- the number of complaints resolved informally, a summary of the types of such complaints so resolved, and the number of covered entities that received technical assistance from the Secretary during such year in order to achieve compliance with such provisions and the types of such technical assistance provided;
- the number of complaints that have resulted in the imposition of civil money penalties (CMPs) or that have been resolved through monetary settlements, including the nature of the complaints involved and the amount paid in each penalty or settlement;
- the number of compliance reviews HHS conducted and the outcome of each such review;
- the number of subpoenas or inquiries issued;
- the number of audits performed and a summary of audit findings pursuant to section 13411 of the HITECH Act; and
- the Secretary's plan for improving compliance with and enforcement of the HIPAA Rules for the following year.

This report is prepared for the calendar year 2018. The Reports to Congress on Compliance with the HIPAA Privacy and Security Rules for previous years are available at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/compliancereptmain.html.

Background

HIPAA was enacted on August 21, 1996. Subtitle F of HIPAA, known as the Administrative Simplification provisions permitted the Secretary to establish standards for the privacy and security of individually identifiable health information held by an entity subject to HIPAA, defined in the HIPAA Rules as a "covered entity." A covered entity is a health plan, a health care provider that electronically transmits any health information in connection with certain financial and administrative transactions (such as electronically billing health insurance carriers for services), or a health care clearinghouse. The HITECH Act, which strengthened HIPAA's privacy and security protections, also expanded the applicability of certain provisions of the HIPAA Rules to business associates of covered entities.[1] A "business associate" is a person or entity, other than a member of the workforce of a covered entity, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve creating, receiving, maintaining, or transmitting protected health information (PHI). Any subcontractor of a business associate that creates, receives, maintains, or transmits PHI on behalf of that business associate is also a business associate.

The HIPAA Privacy Rule, found at 45 CFR Part 160 and Subparts A and E of Part 164, provides important federal protections to protect the privacy of PHI and gives individuals rights with respect to that information. Covered entities and their business associates may not use or disclose PHI, except either as the Privacy Rule permits or requires or as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing.

The HIPAA Security Rule, found at 45 CFR Part 160 and Subparts A and C of Part 164, establishes national standards to protect electronic PHI (ePHI) created, received, used or maintained by covered entities and their business associates. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of ePHI.

The HIPAA Breach Notification Rule, found at 45 CFR Part 160 and Subparts A and D of Part 164, requires HIPAA covered entities to notify affected individuals, the Department, and, in some cases, the media, following the discovery of a breach of unsecured PHI. Business associates are also required to notify covered entities following the discovery of a breach.

For most HIPAA covered entities, compliance with the Privacy Rule was required by April 14, 2003, compliance with the Security Rule was required by April 20, 2005, and compliance with the Breach Notification Rule was required for breaches that occurred on or after September 23, 2009.[2] This report includes information about the Department's enforcement process with regard to the Privacy, Security, and Breach Notification Rules, and information about the Department's efforts to enforce the Rules during the calendar year of 2018.

---

[1] On January 25, 2013, the Department published a final rule that implemented changes required by the HITECH Act and by the Genetic Information Nondiscrimination Act of 2008. Among other things, the final rule extends liability for violations of the HIPAA Security Rule and certain provisions of the HIPAA Privacy Rule to business associates of HIPAA covered entities, effective September 23, 2013.

[2] A separate Report to Congress, available at https://www.hhs.gov/hipaa/for-professionals/breach-notification/reports-congress/index.html, describes the types and numbers of breaches reported to the Secretary and the actions that have been taken by covered entities and business associates in response to the reported breaches.

Enforcement Process

OCR enforces the HIPAA Rules by investigating written complaints filed with OCR, either on paper, by e-mail, or through its complaint portal. OCR also conducts compliance reviews of circumstances brought to its attention to determine if covered entities or business associates are in compliance with the Rules. In addition, OCR's compliance activities include conducting audits[3] and providing education and outreach to foster compliance with the Rules, which are discussed later in the report. When necessary, OCR has authority to issue subpoenas to compel cooperation with an investigation.

Complaints

Under the law, OCR may take action only on complaints that meet the following conditions:

- The alleged violation must have occurred after compliance with the HIPAA Rules was required.

- The complaint must be filed against an entity that is required by law to comply with the HIPAA Rules (i.e., either a covered entity or a business associate).

- The complaint must describe an activity that, if determined to have occurred, would violate the HIPAA Rules.

- The complaint must be filed within 180 days of when the individual submitting the complaint knew or should have known about the act or omission that is the subject of the complaint. OCR may waive this time limit if it determines that the individual submitting the complaint shows good cause for not submitting the complaint within the 180 day time frame (e.g., circumstances that made submitting the complaint within 180 days impossible).

OCR must determine whether a complaint presents an eligible case for enforcement of the HIPAA Rules, as described above. In many cases, OCR lacks jurisdiction under the HIPAA Rules because the complaint alleges a violation by an entity not covered by the HIPAA Rules, describes an activity that would not violate the HIPAA Rules, or the complaint was untimely. In addition, in many cases, OCR provides technical assistance to the covered entity or business associate to resolve the case quickly without further investigation.

Compliance Reviews

OCR may open compliance reviews of covered entities and business associates based on an event or incident brought to the attention of OCR, such as through the media or based upon patterns identified through complaints.

[3] Section 13411 of the HITECH Act, which became effective on February 17, 2010 requires the Department to undertake periodic audits to ensure that covered entities and business associates comply with the HIPAA Rules. As a result of the HITECH Act's mandate, the first phase of the audit program was completed in 2012. The second phase has concluded and OCR is reviewing the results of the previous audits to determine how to implement future audits.

Investigations

Once OCR initiates an investigation, OCR collects evidence through interviews, witness statements, requests for data from the entity involved, site visits, or other available, relevant documents. Covered entities and business associates are required by law to cooperate with complaint investigations and compliance reviews. If a complaint or other event implicates the criminal provision of HIPAA (42 U.S.C. § 1320d-6), OCR may refer the complaint to the Department of Justice (DOJ) for investigation. If DOJ declines to open a case referred by OCR for criminal investigation, OCR reviews the case for potential civil violations of the HIPAA Rules and may investigate the case.

In some cases, OCR may determine, based on the evidence, that there is insufficient evidence to support a finding that a covered entity or business associate violated the HIPAA Rules. In such cases, OCR sends a closure letter to the parties involved explaining the results of the investigation.

In other cases, OCR may determine, based on the evidence, that the covered entity or business associate was not in compliance with the HIPAA Rules. In such cases, OCR will generally first attempt to resolve the case by obtaining voluntary compliance through corrective action, which may include a resolution agreement.

Where corrective action is sought, OCR obtains satisfactory documentation and other evidence from the covered entity or business associate that they undertook the required corrective action to resolve the potential HIPAA violations. In the vast majority of cases, a covered entity or business associate will, through voluntary cooperation and corrective action, be able to demonstrate satisfactory compliance with the HIPAA Rules.

Resolution Agreements

Where OCR finds indications of noncompliance due to willful neglect, or where the nature and scope of the noncompliance warrants additional enforcement action, OCR pursues a resolution agreement with a payment of a settlement amount and an obligation to complete a corrective action plan. In these cases, OCR notifies the covered entity or business associate that, while OCR is prepared to assess a CMP with regard to the potential violations of the HIPAA Rules, OCR is willing to negotiate the terms of a resolution agreement and corrective action plan, to informally resolve the indications of noncompliance. These settlement agreements involve the payment of a monetary amount that is a reduced percentage of the potential CMPs for which the covered entity or business associate would be liable. Additionally, in most cases, the resolution agreement includes a corrective action plan that requires the covered entity or business associate to fix remaining compliance issues; in many cases, the corrective action plan requires them to undergo monitoring of its compliance with the HIPAA Rules for a specified period of time. While this type of resolution still constitutes informal action on the part of OCR, resolution agreements and corrective action plans are powerful enforcement tools for OCR.

Civil Money Penalties

OCR has the discretion to proceed directly to a CMP in an appropriate case, such as one involving particularly egregious circumstances. Further, if OCR and a covered entity or business associate are unable to reach a satisfactory agreement to resolve the matter informally, or if a covered entity or business associate breaches the terms of a resolution agreement, OCR may pursue formal enforcement. In such cases, OCR notifies the covered entity or business associate of a proposed determination of a violation of the HIPAA Rules and OCR's intent to impose a CMP. If a CMP is proposed, the covered entity or business associate may request a hearing in which a Departmental administrative law judge decides if the CMP is supported by the evidence in the case.

Audits

Section 13411 of the HITECH Act requires HHS to perform periodic audits of covered entity and business associate compliance with the HIPAA Rules.

These audits are reviews of covered entities and business associates that are initiated not because of any particular event or incident indicating possible noncompliance on the part of the covered entity or business associate, but rather based on application of a set of objective selection criteria. The objective of the audits is to (1) assess an entity's effort to comply with the HIPAA Rules, (2) ensure covered entities and business associates are adequately safeguarding PHI, and (3) ensure individuals are provided the rights afforded to them by the HIPPA Rules.

Summary of Complaints and Compliance Reviews

As discussed in greater detail below, in addition to requiring covered entities and business associates to take corrective action in hundreds of cases, for 2018, the Department resolved eleven investigations with resolution agreements/corrective action plans or the imposition of civil money penalties totaling more than $28 million.

Enforcement Data

Complaint Resolutions

2018 Complaints

During calendar year 2018, OCR received 25,912 new complaints and carried over approximately 3,909 cases from 2017. OCR resolved 25,089 complaints during calendar year 2018.

In 2018, OCR resolved 16,989 cases (68%) before initiating an investigation. Examples of pre-investigation closures include complaints that alleged violations by an entity not covered by the HIPAA Rules, described activities that did not violate the HIPAA Rules, or were untimely. OCR resolved 6,912 cases (28%) by providing technical assistance in lieu of an investigation.

OCR completed investigations in 1,188 cases. For 632 of these cases, OCR required the covered entity or business associate to take corrective action (53% of the complaints investigated); for 289 of these cases, OCR provided technical assistance after initiating an investigation (24% of the complaints investigated). In 267 cases investigated (22% of the complaints investigated), OCR found that insufficient evidence that a violation of the HIPAA Rules had occurred. See Figure 1.

COMPLAINT ENFORCEMENT RESULTS
JANUARY 1, 2018 THROUGH DECEMBER 31, 2018

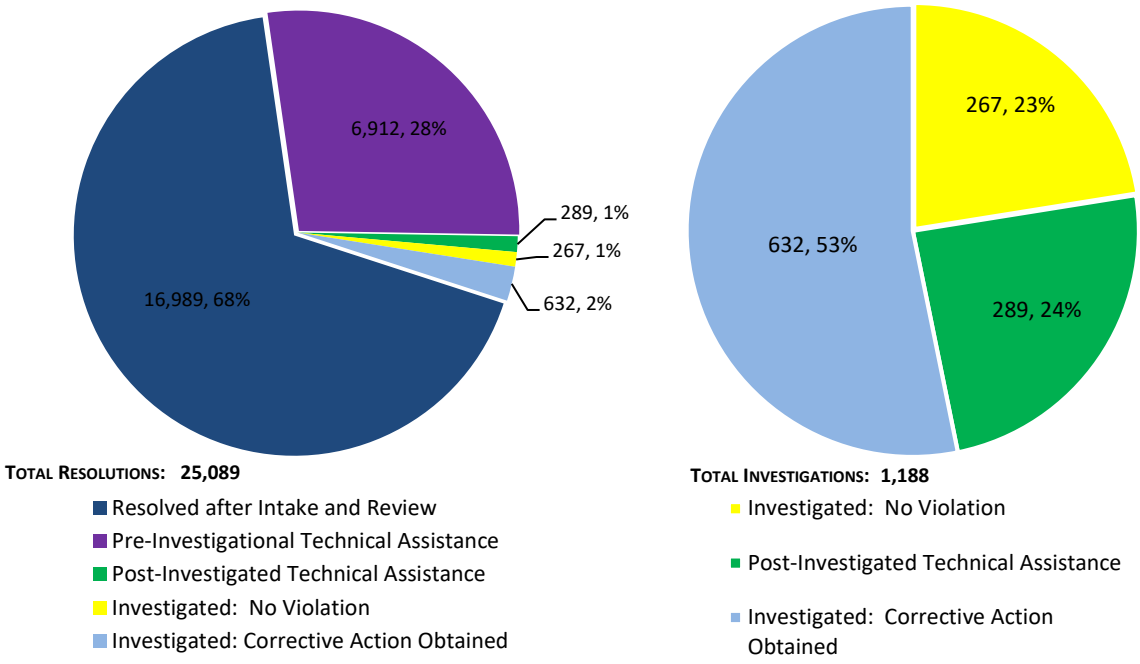

Figure 1

OCR received 25,912 complaints in 2018. Of these cases, three were resolved in 2018 through resolution agreements/corrective action plans and monetary settlements totaling $336,400.[4] No complaints were resolved by assessing CMPs.[5]

For the 25,089 complaints OCR resolved in 2018, the top five issues were Impermissible Uses and Disclosures, Safeguards, Administrative Safeguards (Security Rule), Right of Access, and Technical Safeguards (Security Rule). These issues accounted for eight percent of resolved complaints.

OCR received 1,409 more complaints in 2018 than in 2017, an increase of six percent (24,503 cases received in 2017, compared to 25,912 cases received in 2018).

[4] The three cases that were resolved are Filefax, Allergy Associates of Hartford, and Pagosa Springs Medical Center. See Appendix for additional information.
[5] One breach investigation was the subject of a hearing with an Administrative Law Judge. The ALJ confirmed imposition of CMPs of $4.3 million. MD Anderson appealed the ALJ decision, HHS prevailed at the Departmental Appeals Board, and the matter is currently pending in the U.S. Court of Appeals for the Fifth Circuit. See Appendix for additional information.

Compliance Reviews

2018 Compliance Reviews

During calendar year 2018, OCR opened 447 compliance reviews addressing allegations of violations of the HIPAA Rules that did not arise from complaints.[6] Of these, 376 compliance reviews were a result of a breach report affecting 500 or more individuals and 17 were a result of a breach report affecting fewer than 500 individuals. The remaining 54 compliance reviews were opened based on incidents brought to OCR's attention through other means.

OCR closed 438 compliance reviews in 2018. Of the closed cases, 431 originated from breach reports and 7 originated from other means. The covered entity or business associate took corrective action or paid a CMP in 363 cases (83%). The covered entity or business associate was provided technical assistance after investigation in 42 cases (10%). OCR found that there was insufficient evidence of a violation of the HIPAA Rules in 17 cases (4%). OCR determined that it did not have jurisdiction to investigate the allegations in 10 cases (2%). OCR closed compliance reviews without requiring corrective actions or making recommendations in six cases (1%). Of the completed compliance reviews, three cases were resolved through monetary settlements totaling $999,000. See Figure 2.

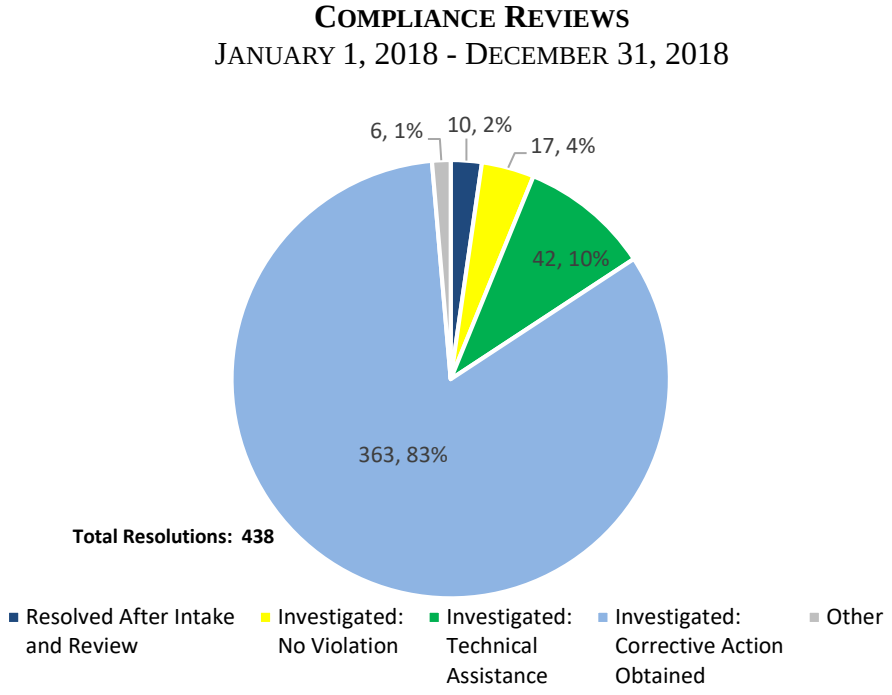

Figure 2

[6] Compliance reviews are opened for all reports of breaches affecting 500 or more individuals, and for some reports of breaches affecting fewer than 500 individuals.

Subpoenas

OCR did not issue any subpoenas in 2018.

Audits

The audited provisions were selected for Phase 2 based on the results from the 2012 audits and more recent OCR enforcement activities, which identified weakness in entity implementation in certain areas. Covered entities and business associates were asked to submit documentation of their compliance. Covered entities were audited either on the provisions of the Privacy and Breach Notification Rules or the Security Rule. Business associate were audited on either the provisions of the Breach Notification or the Security Rule.

The covered entity audits examined:

- Risk analysis and risk management policies, procedures and activities pursuant to the Security Rule;
- The content and timeliness of notifications made pursuant to the Breach Notification Rule; and
- The electronic posting of Notices of Privacy Practices and the provision of individual access to health information pursuant to the Privacy Rule.

The business associate audits examined:

- Risk analysis and risk management policies, procedures and activities pursuant to the Security Rule; and
- The timeliness of breach incident reporting to covered entities pursuant to the Breach Notification Rule.

Results

- The majority of audited covered entities issued breach notifications to individuals within the regulatory timeframe.
- Most audited covered entities prominently posted their Notices of Privacy Practices on their websites.
- Covered entities are not consistently providing individuals with access to their medical records.
- Notices of Privacy Practices often were missing required elements, such as uses and disclosures requiring an opportunity for an individual to agree or object (or requiring the entity's best judgement). Adapting an HHS model notice would avoid that mistake.

- Most audited entities, both covered entities and business associates, failed to safeguard PHI by implementing adequate risk analysis and risk management measures.
- More than three-quarters of the audited business associates stated that they had never experienced a breach of PHI. Many did not understand that they had breach notification responsibilities under the HIPAA Rules.

OCR expects to release a final report on the findings of the audit program in 2020. This report will present information about OCR's Phase 2 audits, the achievements and weaknesses identified and methods audited entities may implement to strengthen compliance. The report will identify technical assistance and resources for covered entities and business associates to improve compliance with the HIPAA Rules.

Secretary's Plan for Improving Compliance – Ongoing Outreach Efforts to Increase Awareness and Compliance

OCR continued to build its public outreach and education efforts in support of the HITECH Act's mandate to increase education to both HIPAA covered entities and consumers, and to address compliance deficiencies in the regulated community that have been identified by complaint investigations, compliance reviews, and the audit program. In 2018, OCR continued its work to help consumers better understand their HIPAA rights and to provide the regulated community with technical assistance and best practices that promote better compliance with the HIPAA Rules. OCR's 2018 outreach efforts include:

- OCR amplified the second phase of its "Information is Powerful Medicine" campaign to help raise awareness about the HIPAA right to access health information, and to empower individuals to better participate in their own medical care. Activities included dissemination of print materials to partners of the All of Us Research Program at the National Institutes of Health, digital media buys, and outdoor transit ads to drive traffic to the campaign website at http://www.hhs.gov/getitcheckituseit. The website provides links to factsheets, videos, and key messages to enable individuals to better understand their HIPAA rights to see and get copies of their health information.
- In October 2018, OCR renewed its popular on-line provider education training that enables health care professionals to obtain free continuing medical education and continuing education credits on key aspects of, and their legal responsibilities under HIPAA and how the individual's right to obtain their health information assists individuals to become more involved in their own care. OCR has trained approximately 56,000 professionals from October 2017 through December 2018.
- Throughout 2018, OCR collaborated with partner agencies within HHS to identify and develop model programs and materials for training healthcare providers, patients, and their families regarding permitted uses and disclosures of the PHI of patients seeking or undergoing mental health or substance use disorder treatment, and to develop a plan to share the programs and materials with professionals and consumers. Activities included a webinar for providers with the Centers for Medicare & Medicaid Services; an in-depth training to the Mental Health Liaison Group (MHLG), a coalition of national organizations representing consumers, family members, mental health and addiction

providers, advocates, payers and other stakeholders committed to strengthening Americans' access to mental health and addiction care; and OCR's regional offices have presented across the country on OCR's HIPAA guidance on mental health and substance abuse disorder.

- OCR's redesigned, plain language website continues to provide both consumers and professionals with easy to find information on the HIPAA Privacy, Security and Breach Notification Rules. Web content is updated regularly to ensure that information is fresh and relevant. According to Google Analytics, OCR's HIPAA pages receive over 300,000 unique visits a month.

- In 2018, OCR co-hosted its 11th annual "Safeguarding Health Information: Building Assurance through HIPAA Security" conference with the National Institute for Standards and Technology. The two-day annual conference explored the current health information technology security landscape, and offered practical strategies, tips and techniques for complying with the HIPAA Security Rule. Attendees participated on-site and through a live webcast, with 250 attending in person and over 1200 via web.

- Throughout 2018, OCR continued its series of cybersecurity newsletters to better inform the regulated community of the various security threats and vulnerabilities that currently exist in the healthcare sector, to understand what security measures can be taken to decrease the possibility of being exposed by these threats, and how to reduce breaches of ePHI. OCR published 9 newsletters on a variety of topics to provide best practices and other practical information to help HIPAA covered entities and business associates practice better cyber hygiene.

- OCR collaborated with the Office of the National Coordinator for Health Information Technology (ONC) to develop and disseminate a set of easy-to-understand educational tools to ensure that patients and other participants in the health care system understand the individual's right to access their health information, and how to exercise that right. The Guide to Getting & Using Your Health Record, which supports the Department's responsibilities under section 4006 of the 21st Century Cures Act to promote the right of access through public education, is available at https://www.healthit.gov/how-to-get-your-health-record/.

Appendix

Significant Activities: Resolution Agreements and Civil Money Penalties (CMPs)[7] in 2018

Resolution Agreement with Fresenius Medical Care North America

Fresenius Medical Care North America (FMCNA) agreed to settle potential violations of the HIPAA Privacy and Security Rules with OCR. FMCNA paid $3.5 million and agreed to adopt a corrective action plan to correct deficiencies in its HIPAA compliance program. FMCNA is a provider of products and services for people with chronic kidney failure, with over 60,000 employees that serve over 170,000 patients. FMCNA's network is comprised of dialysis facilities, outpatient cardiac and vascular labs, and urgent care centers, as well as hospitalist and post-acute providers.

On January 21, 2013, FMCNA filed five separate breach reports for separate incidents occurring between February 23, 2012, and July 18, 2012, implicating the ePHI of five separate FMCNA owned covered entities.

OCR's subsequent investigation found 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;
- Impermissibly disclosed ePHI without an authorization;
- Failed to implement policies and procedures to address security incidents;
- Failed to implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI;
- Failed to implement a mechanism to encrypt and decrypt ePHI; and
- Failed to safeguard its facilities and equipment for unauthorized access, tampering, and theft.

In addition to a $3.5 million settlement, FMCNA agreed to:

- Complete a risk analysis and risk management plan to comply with the HIPAA Privacy and Security Rule;
- Revise policies and procedures to comply with the HIPAA Security Rule; and
- Train workforce members on the revised policies and procedures.

This settlement occurred in January 2018.

[7] Information provided here on Resolution Agreements and CMPs are based on the year in which the Agreement was signed or the CMP assessed. Investigations of these cases were initiated in years prior to 2018.

Resolution Agreement with Filefax

A receiver appointed to liquidate the assets of Filefax, Inc. paid $100,000 to settle potential violations of the HIPAA Privacy Rule. Filefax, located in Northbrook, Illinois, provided for the storage, maintenance, and transportation of medical records for covered entities.

On February 10, 2015, OCR received an anonymous complaint alleging that an individual transported medical records obtained from Filefax to a shredding and recycling facility to sell. The medical records contained patients' PHI.

OCR's investigation found that Filefax:

- Impermissibly disclosed the PHI of 2,150 individuals; and
- Granted permission to an unauthorized person to view and remove PHI.

Filefax is no longer in business. In 2016, a court in unrelated litigation appointed a receiver to liquidate its assets for distribution to creditors and others. In addition to the $100,000 monetary settlement, the receiver agreed, on behalf of Filefax, to properly store and dispose of the remaining medical records found at Filefax's facility in compliance with HIPAA.

This settlement occurred in January 2018.

Civil Money Penalty imposed on The University of Texas MD Anderson Cancer Center (CMP)

A HHS Administrative Law Judge (ALJ) ruled that The University of Texas MD Anderson Cancer Center (MD Anderson) violated the HIPAA Privacy and Security Rules and granted judgment to OCR on all issues, and confirmed the imposition of a CMP on MD Anderson in the amount of $4,348,000. This is the second judgment in OCR's history of HIPAA enforcement.

MD Anderson is both a degree-granting academic institution and a comprehensive cancer treatment and research center located at the Texas Medical Center in Houston. 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 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 implement encryption of 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. The ALJ agreed with OCR's findings and the CMP.

The ALJ issued a decision upholding the CMP in June 2018. MD Anderson appealed the ALJ's decision, which was subsequently affirmed. MD Anderson filed an appeal with the U.S. Court of Appeals for the Fifth Circuit, which is currently pending.

Resolution Agreement with Boston Medical Center (BMC), Brigham and Women's Hospital (BWH), and Massachusetts General Hospital (MGH)

Boston Medical Center (BMC), Brigham and Women's Hospital (BWH), and Massachusetts General Hospital (MGH) agreed to settle potential violations of the HIPAA Privacy Rule. Collectively, the three entities paid $999,000 for compromising the privacy of patients' PHI by inviting film crews onto their premises to film an ABC television network documentary series, without first obtaining authorization from patients.

OCR's investigation found that BMC, BWH, and MGH:

- Impermissibly disclosed the PHI of numerous patients; and
- Failed to appropriately safeguard their patients' PHI from disclosure.

To resolve potential HIPAA violations, BMC paid OCR $100,000, BWH paid $384,000, and MGH paid $515,000. Additionally, each entity agreed to:

- Develop, maintain, and revise if necessary written policies and procedures to comply with the HIPAA Privacy Rule; and
- Train workforce members on the revised policies and procedures.

The settlement with BMC occurred in August 2018. The settlements with BWH and MGH occurred in September 2018.

Resolution Agreement with Anthem

Anthem, Inc. agreed to pay $16 million and take substantial corrective action to settle potential violations of the HIPAA Privacy and Security Rules after a series of cyberattacks led to the largest U.S. health data breach in history and exposed the ePHI of almost 79 million people. The $16 million settlement is nearly three times the previous high of $5.55 million paid to OCR in 2016.

Anthem is an independent licensee of the Blue Cross and Blue Shield Association operating throughout the United States and is one of the nation's largest health benefits companies, providing medical care coverage to one in eight Americans through its affiliated health plans. This breach affected the ePHI that Anthem, Inc. maintained for its affiliated health plans and many other covered entity health plans.

On March 13, 2015, Anthem filed a breach report with OCR, stating that it discovered cyber-attackers had gained access to its IT system via an undetected continuous and targeted cyberattack for the apparent purpose of extracting data. Anthem discovered cyber-attackers had infiltrated its 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 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.

Further, OCR's investigation found that Anthem:

- Failed to implement appropriate measures for detecting hackers to prevent, detect, contain, and correct security violations;
- Failed to implement strong password policies and procedures;
- Failed to monitor and respond to security incidents in a timely fashion;
- Failed to conduct an enterprise-wide risk analysis; and
- Failed to implement adequate minimum access controls to prevent access to sensitive ePHI.

In addition to the $16 million settlement, Anthem will undertake a robust corrective action plan to comply with the HIPAA Rules. Anthem also agreed to:

- Develop, maintain, and revise if necessary written policies and procedures to comply with the HIPAA Privacy Rule;
- Train workforce members on the revised policies and procedures; and
- Post a copy of the revised policies and procedures on its intranet.

This settlement occurred in October 2018.

Resolution Agreement with Allergy Associates of Hartford

Allergy Associates of Hartford, P.C., agreed to settle violations of the HIPAA Privacy Rule with OCR. Allergy Associates is a health care practice that specializes in treating individuals with allergies, and is comprised of three doctors at four locations across Connecticut. Allergy Associates paid $125,000 and agreed to the adoption and implementation of a corrective action plan and monitoring of its compliance efforts for a two-year period.

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. The reporter subsequently contacted the doctor for comment and the doctor impermissibly disclosed the patient's PHI to the reporter.

OCR's investigation found that Allergy Associates:

- Failed to take any disciplinary action against the doctor for the unauthorized disclosure of PHI; and
- Did not take any corrective action following the impermissible disclosure to the media.

In addition to the $125,000 settlement, Allergy Associates agreed to:

- Develop, maintain, review, and revise, if necessary, HIPAA Privacy Rule policies and procedures; and
- Train workforce members on HIPAA Privacy Rule policies and procedures.

This settlement occurred in October 2018.

Resolution Agreement with Advanced Care Hospitalists

Advanced Care Hospitalists PL (ACH) agreed to pay $500,000 and adopt a substantial corrective action plan to settle potential violations of the HIPAA Privacy and Security Rules. ACH provides contracted internal medicine physicians to hospitals and nursing homes in Florida. ACH provided services to more than 20,000 patients annually and employed between 39 and 46 individuals during the relevant timeframe.

Between November 2011 and June 2012, ACH engaged the services of an individual that presented himself as a representative of a Florida-based company named Doctor's First Choice Billings, Inc. (First Choice). The individual provided medical billing services to ACH using First Choice's name and website, but allegedly without any knowledge or permission of First Choice's owner.

On February 11, 2014, a local hospital notified ACH that patient information was viewable on the First Choice website, including name, date of birth, and social security number. In response, ACH was able to identify at least 400 affected individuals and asked First Choice to remove the PHI from its website. ACH filed a breach notification report with OCR on April 11, 2014, stating that 400 individuals were affected; however, after further investigation, ACH filed a supplemental breach report stating that an additional 8,855 patients could have been affected.

OCR's investigation found that ACH:

- Failed to enter into a business associate agreement with the medical billing service as required by HIPAA;
- Failed to adopt policies requiring business associate agreements until April 2014; and
- Failed to conduct a risk analysis or implement security measures.

In addition to the monetary settlement, ACH agreed to:

- Adopt and implement business associate agreements with all vendors;
- Complete an enterprise-wide risk analysis; and
- Develop comprehensive policies and procedures to comply with the HIPAA Rules.

This settlement occurred in September 2018.

Resolution Agreement with Pagosa Springs Medical Center

Pagosa Springs Medical Center (PSMC) paid $111,400 to settle potential violations of the HIPAA Privacy and Security Rules. PSMC is a critical access hospital that provides medical services in Colorado and employs more than 175 individuals.

The settlement resolves a complaint alleging that a former PSMC employee 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
- Impermissibly disclosed the ePHI of 557 individuals to the web-based scheduling calendar vendor without a business associate agreement in place.

In addition to the $111,400 settlement amount, PSMC agreed to:

- Revise and update its security management plan;
- Adopt and implement a business associate agreement;
- Revise its policies and procedures to comply with the HIPAA Privacy and Security Rules; and
- Train workforce members on HIPAA Privacy and Security Rules' policies and procedures.

This settlement occurred in November 2018.

Resolution Agreement with Cottage Health

Cottage Health agreed to pay $3 million and adopt a substantial correction action plan to settle potential violations of the HIPAA Security Rules. Cottage Health operates Santa Barbara Cottage Hospital, Santa Ynez Cottage Hospital, Goleta Valley Cottage Hospital, and Cottage Rehabilitation Hospital, in California. OCR received two notifications from Cottage Health regarding breaches of unsecured ePHI affecting over 62,500 individuals, one in December 2013 and another in December 2015.

The first breach arose when ePHI on a Cottage Health server was accessible from the Internet. OCR's investigation determined that security configuration settings of the Windows operating system permitted access to files containing ePHI without requiring a username and password. As a result, patient names, addresses, dates of birth, diagnoses, conditions, lab results and other treatment information were available to anyone with access to Cottage Health's server. The second breach occurred when a server was misconfigured following an IT response to a troubleshooting ticket, exposing unsecured ePHI over the Internet. This ePHI included patient names, addresses, dates of birth, social security numbers, diagnoses, conditions, 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 an appropriate level;
- Failed to perform periodic technical and non-technical 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.

In addition to the monetary settlement, Cottage Health agreed to:

- Conduct an enterprise-wide risk analysis;
- Develop a risk management plan;
- Implement processes for the evaluation of environmental and operational changes;
- Implement and distribute policies and procedures for protecting PHI; and
- Train all workforce members who have access to PHI.

This settlement occurred in December 2018.