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

For Calendar Year 2019

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 Secretary) to prepare and submit an annual report to the Senate Committee on Health, Education, Labor, and Pensions, the House Committee on Ways and Means, and the House Committee on Energy and Commerce (the Committees), regarding "complaints alleging violations of law, including the provisions [of the HITECH Act] as well as the provisions of [the Privacy and Security Rules promulgated under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Pub. L. 104-191)] relating to privacy and security of health information that is received by the Secretary during the year for which the report is being prepared."

Section 13424(a)(1) of the HITECH Act requires that the report include:

- the number of complaints received by the U.S. Department of Health and Human Services (HHS or the Department) from the public;
- the number of such 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 such 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 review;
- the number of subpoenas or inquiries issued;
- the Secretary's plan for improving compliance with and enforcement of the HIPAA Rules for the following year; and
- the number of audits performed and a summary of audit findings pursuant to section 13411 of the HITECH Act.

This report is prepared for the calendar year 2019. 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 (the HIPAA Rules),

[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.

and information about the Department's actions to enforce the HIPAA Rules during the calendar year of 2019.

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 HIPAA Rules. In addition, OCR's compliance activities include conducting audits[3] and providing education and outreach to support compliance with the HIPAA 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

[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 concluded in 2018. OCR is reviewing the results of the previous audits to determine how to implement future audits.

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

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 it undertook the required corrective action to resolve the potential HIPAA violation(s). 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 (CAP). 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 CAP 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 could be liable. Additionally, in most cases, the resolution agreement includes a CAP that requires the covered entity or business associate to fix remaining compliance issues; and the CAP 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 CAPs are powerful enforcement tools for OCR, as they provide a specific deterrent for noncompliance with the HIPAA Rules for entities under investigation, and a general deterrent to the regulated industry when OCR announces a resolution.

Civil Money Penalties

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. If the covered entity or business associate does not request a hearing within 90 days of receipt of OCR's proposed determination, OCR will issue a final determination and a CMP.

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 that covered entities and business associates are adequately safeguarding PHI, and 3) ensure that individuals are provided the rights afforded to them by the HIPAA Rules.

OCR did not initiate any audits in 2019 and is currently preparing for the next round of audits. The first phase of our audit program was completed in 2012. Phase II was completed in 2018. In 2020, OCR issued a final report on the findings of the Phase II audits, the achievements and weaknesses identified, and methods audited entities may implement to strengthen compliance.

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 2019, the Department resolved ten investigations with resolution agreements/CAPs or the imposition of CMPs totaling more than $12 million in collections.

Complaint Resolutions

2019 Complaints

During calendar year 2019, OCR received 28,261 new complaints and carried over 3,200 open complaints from 2018. OCR resolved 29,853 complaints during calendar year 2019.[4] Of those, OCR resolved 19,584 (66%) before initiating an investigation. Examples of pre-investigation closures include complaints that alleged violations by an entity not covered by the HIPAA Rules and allegations involving conduct that did not violate the HIPAA Rules or were untimely. OCR resolved 8,770 complaints (29%) by providing technical assistance in lieu of an investigation.

OCR completed investigations in 1,499 complaints.[5] In 803 of these complaints, OCR required the covered entity or business associate to take corrective action (53% of the complaints investigated); in 252 of these complaints, OCR provided technical assistance after initiating an investigation (17% of the complaints investigated). In 444 of the complaints OCR investigated (30% of the complaints investigated), it found insufficient evidence that a violation of the HIPAA Rules had occurred. See Figure 1.

COMPLAINT ENFORCEMENT RESULTS
JANUARY 1, 2019, THROUGH DECEMBER 31, 2019

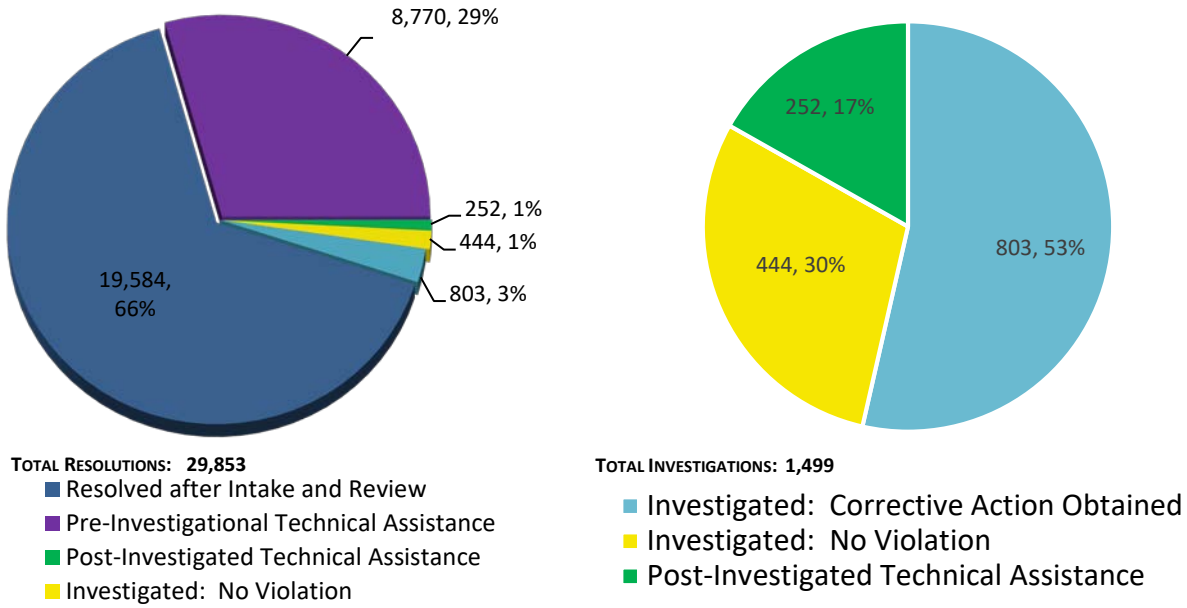

Figure 1

[4] The new complaints received and complaints resolved in a calendar year are not the same as OCR has complaint investigations that carry over from the previous year and are not counted as new complaints received when they are closed in a subsequent calendar year.
[5] The number of complaints resolved in a given calendar year is the sum of administrative closures, technical assistance closures and investigated closures.

OCR resolved four complaint investigations in 2019 through resolution agreements/CAPs and monetary settlements totaling $2,355,000.[6] No complaints were resolved by assessing CMPs.[7]

For the 29,853 complaints OCR resolved in 2019, the top five issues alleged were Impermissible Uses and Disclosures (928 complaints), Safeguards (809 complaints), Right of Access (340 complaints), Administrative Safeguards (Security Rule) (318 complaints), and Minimum Necessary (195 complaints). OCR received 2,349 more complaints in 2019 than in 2018, an increase of nine percent (OCR received 25,912 complaints in 2018, compared to 28,261 complaints in 2019).

Compliance Reviews

2019 Compliance Reviews

During calendar year 2019, OCR initiated 611 compliance reviews to investigate allegations of violations of the HIPAA Rules that did not arise from complaints.[8] Of these, 522 compliance reviews were initiated as a result of a breach report affecting 500 or more individuals and 20 were a result of a breach report affecting fewer than 500 individuals. The remaining 69 compliance reviews were opened based on incidents brought to OCR's attention through anonymous complaints, media reports, or other means.

OCR closed 338 compliance reviews in 2019.[9] Of the closed cases, 298 originated from breach reports and 40 originated from other means. The covered entity or business associate took corrective action or paid a CMP in 252 cases (75%). The covered entity or business associate was provided technical assistance after investigation in 38 cases (11%). OCR found that there was insufficient evidence of a violation of the HIPAA Rules in 43 cases (13%). OCR determined that it did not have jurisdiction to investigate the allegations in 5 cases (1%). Of the completed compliance reviews (338), four cases were resolved through monetary settlements totaling $6,165,000;[10] and two cases were resolved through CMPs totaling $3,754,000.[11] See Figure 2.

[6] The four complaints that were resolved are Bayfront Health St. Petersburg, Elite Dental Associates-Dallas, Sentara Hospitals, and Korunda Medical. See Appendix for additional information.
[7] Two breach investigations were resolved through the imposition of CMPs. See Appendix for additional information.
[8] 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.
[9] The new compliance reviews initiated, and compliance reviews resolved in a calendar year are not the same as OCR has compliance review investigations that carry over from the previous year and are not counted as new compliance reviews initiated when they are closed in a subsequent calendar year.
[10] The four cases that were resolved are Touchstone Medical Imaging, Medical Informatics Engineering, University of Rochester Medical Center, and West Georgia Ambulance.
[11] OCR's imposition of a CMP in the Jackson Health System investigations resolved two breach reports submitted by Jackson Health System and a compliance review initiated by OCR. The other case resolved via CMP was the Texas Health and Human Services Commission case.

COMPLIANCE REVIEWS
JANUARY 1, 2019 – DECEMBER 31, 2019

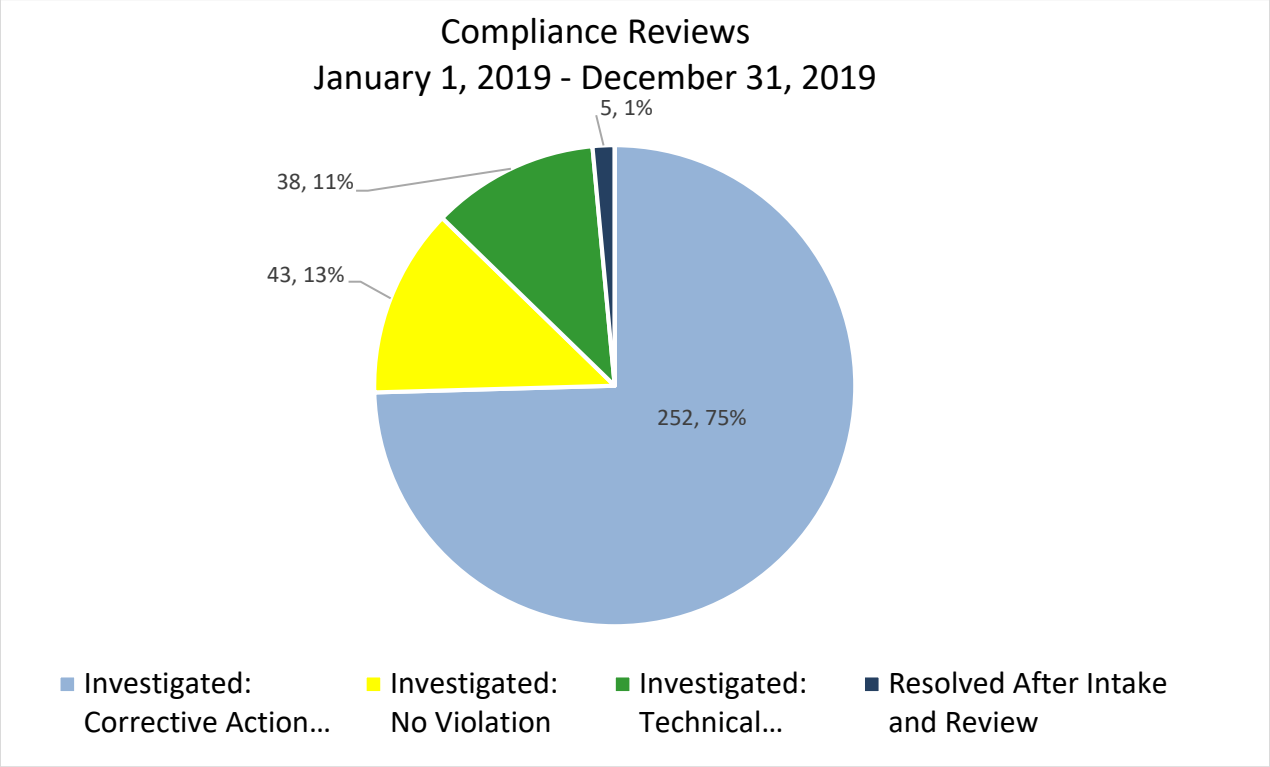

Figure 2

Subpoenas

OCR did not issue any subpoenas in 2019.

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. OCR's 2019 outreach highlights include:

- In October 2019, OCR co-hosted its 12th annual "Safeguarding Health Information: Building Assurance through HIPAA Security" conference with the National Institute for Standards and Technology. The two-day annual conference featured a timely update and overview from the OCR Director. Panels and presentations addressed the latest thinking on enterprise-wide risk management; emerging cybersecurity threats to the healthcare industry; management of medical devices, applications, and Internet of Things (IoT) in

healthcare environments; and updates from other federal healthcare agencies with best practices for complying with the HIPAA Security Rule. The conference continues to grow in popularity, with over 200 attendees participating on-site and over 8,000 views of the live webcast.

- In 2019, OCR continued to offer its popular on-line provider education training through Medscape 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 an individual's right to obtain their health information assists individuals in becoming more involved in their own care. OCR trained 30,448 learners from January 2019 through December 2019.

- OCR's redesigned, plain language website continues to provide consumers and professionals with easy to find information on the HIPAA Rules. Web content is updated regularly to ensure that information is fresh and relevant. According to Google Analytics, OCR's HIPAA pages received over 300,000 unique visits a month in 2019.

- OCR continues to provide cybersecurity newsletters to help HIPAA covered entities and business associates remain in compliance with the HIPAA Security Rule by identifying emerging or prevalent issues and highlighting best practices to safeguard PHI. 2019 topics included Managing Malicious Insider Threats; Advanced Persistent Threats and Zero Day Vulnerabilities; and Preventing, Mitigating and Responding to Ransomware.

- In 2019, OCR continued its collaboration with the Office of the National Coordinator for Health Information Technology (ONC) to develop and disseminate an advertising campaign focused on an individual's right to access under HIPAA to their health information. In 2019, the campaign resulted in 17,394,643 impressions[12] and 79,255 unique visits to the campaign's website, https://www.healthit.gov/how-to-get-your-health-record/, featuring a set of easy-to-understand educational tools including *The Guide to Getting & Using Your Health Records*. These efforts continued to support the Department's responsibilities under Section 4006 of the 21st Century Cures Act to promote the HIPAA Right of Access through public education, which also included: distribution of brochures, posters, digital media, and transit advertisement buys as part of OCR's *Information is Powerful Medicine* campaign;[13] outreach slide sets used in OCR and ONC speaking events; OCR health care provider trainings through Medscape; ONC's *Patient Engagement Playbook;* [14] and OCR's Right of Access Enforcement Initiative, which OCR uses to educate regulated entities and the public about the requirements of the Right of Access and to draw attention to the importance of compliance.[15]

[12] Impressions are the number of times elements of a web page are rendered on someone's screen.
[13] The campaign materials are available on the HHS.gov website at http://www.hhs.gov/GetItCheckItUseIt.
[14] The *Patient Engagement Playbook* is available at https://www.healthit.gov/playbook/pe/.
[15] Information about the Right of Access Initiative settlements reached in 2019 is available at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/bayfront/index.html and https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/korunda/index.html.

- In October 2018, OCR and ONC updated the popular Security Risk Assessment (SRA) Tool with a number of enhancements to make it easier to use and apply more broadly to the risks to health information. The tool is designed for use by small to medium sized health care practices and business associates to help them identify risks and vulnerabilities to ePHI. The updated tool provides enhanced functionality to document how such organizations can implement or plan to implement appropriate security measures to protect ePHI. Throughout 2019, OCR and ONC held three webinars to illustrate and promote the tool's use. Each of the webinars reached capacity of 3,000 participants. Due to popularity and demand, OCR and ONC made an encore presentation of this training available in August 2019 on YouTube, which has gained an additional 1,996 views as of December 31, 2019.

Audits

OCR did not initiate any audits in 2019.

Appendix

Significant Activities: Resolution Agreements and Civil Money Penalties (CMPs)[16] in 2019

Resolution Agreement with Touchstone Medical Imaging

Touchstone Medical Imaging (Touchstone) agreed to pay $3 million and take corrective action to settle potential violations of the HIPAA Privacy, Security, and Breach Notification Rules. Touchstone, based in Franklin, Tennessee, provides diagnostic medical imaging services in Nebraska, Texas, Colorado, Florida, and Arkansas.

In May 2014, Touchstone was notified by the Federal Bureau of Investigation (FBI) and OCR that one of its FTP servers allowed uncontrolled access to its patients' PHI. This uncontrolled access permitted search engines to index the PHI of Touchstone's patients, which remained visible on the Internet even after the server was taken offline.

Touchstone initially claimed that no patient PHI was exposed. However, during OCR's investigation, Touchstone subsequently admitted that the PHI of more than 300,000 patients was exposed, including patient names, birth dates, social security numbers, and addresses. OCR's investigation found that Touchstone:

- Failed to thoroughly investigate the security incident until several months after notice of the breach from both the FBI and OCR;
- Failed to notify affected individuals in a timely manner;
- Failed to conduct an accurate and thorough risk analysis of potential risks and vulnerabilities to the confidentiality, integrity, and availability of its electronic PHI (ePHI); and
- Failed to enter into a business associate agreement with its IT support vendor and third-party data center provider as required by HIPAA.

In addition to the monetary settlement, Touchstone agreed to:

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

This settlement occurred in April 2019.

[16] 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 2019.

Resolution Agreement with Medical Informatics Engineering

Medical Informatics Engineering, Inc. (MIE) agreed to pay $100,000 and take corrective action to settle potential violations of the HIPAA Privacy and Security Rules. MIE is an Indiana company that provides software and electronic medical record services to healthcare providers.

On July 23, 2015, MIE filed a breach report with OCR following discovery that hackers used a compromised user ID and password to access the ePHI of approximately 3.5 million people.

OCR's investigation revealed that MIE failed to conduct a comprehensive risk analysis to assess the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its ePHI.

In addition to the monetary settlement, MIE agreed to:

- Complete an enterprise-wide risk analysis; and
- Develop and implement a risk management plan.

This settlement occurred in April 2019.

Resolution Agreement with Bayfront Health St. Petersburg

Bayfront Health St. Petersburg (Bayfront) agreed to pay $85,000 and take corrective action to settle a potential violation of the right of access provision of the HIPAA Privacy Rule after Bayfront failed to provide a mother timely access to records about her unborn child. Bayfront, based in St. Petersburg, Florida, is a Level II trauma and tertiary care center licensed as a 480-bed hospital with over 550 affiliated physicians.

OCR initiated its investigation based on a complaint from the mother. As a result of OCR's investigation, Bayfront directly provided the mother with the requested health information more than nine months after the initial request. The HIPAA Privacy Rule generally requires covered health care providers to provide medical records within 30 days of the request and requires that providers only charge a reasonable cost-based fee. This right to patient records extends to parents who seek medical information about their minor children.

In addition to the monetary settlement, Bayfront agreed to:

- Develop right of access policies and procedures to comply with the HIPAA Privacy Rule;
- Identify business associates that are involved in HIPAA right of access requests and copies of business associate agreements; and
- Train all workforce members and relevant business associates on revised policies and procedures.

This settlement occurred in September 2019.

Resolution Agreement with Elite Dental Associates-Dallas

Elite Dental Associates, Dallas (Elite) agreed to pay $10,000 and take corrective action to settle potential violations of the HIPAA Privacy Rule. Elite is a privately-owned dental practice located in Dallas, Texas, providing general, implant, and cosmetic dentistry.

On June 5, 2016, OCR received a complaint from an Elite patient alleging that Elite had responded to a social media review by disclosing the patient's last name and details of the patient's health condition. OCR's investigation found that Elite:

- Impermissibly disclosed the PHI of multiple patients in response to patient reviews on the Elite Yelp review page;
- Did not have a policy and procedure regarding disclosures of PHI to ensure that its social media interactions protected the PHI of its patients; and
- Did not have a Notice of Privacy Practices that complied with the HIPAA Privacy Rule.

OCR accepted a substantially reduced settlement amount in consideration of Elite's size, financial circumstances, and cooperation with OCR's investigation.

In addition to the monetary settlement, Elite agreed to:

- Develop and adopt policies and procedures regarding the uses and disclosures of PHI;
- Develop and disseminate a Notice of Privacy Practices;
- Train its workforce members on the requirements to maintain patient privacy and confidentiality;
- Issue breach notices to any individuals or their personal representatives whose PHI was disclosed by Elite without a valid authorization; and
- Submit to HHS breach reports regarding the aforementioned individuals or personal representatives notified of a breach.

This settlement occurred in September 2019.

Civil Money Penalty imposed on Jackson Health System

OCR imposed a civil money penalty of $2,154,000 against Jackson Health System (JHS) for violations of the HIPAA Security and Breach Notification Rules between 2013 and 2016. JHS is a nonprofit academic medical system based in Miami, Florida, which operates six major hospitals, a network of urgent care centers, multiple primary care and specialty care centers, long-term care nursing facilities, and corrections health services clinics. JHS provides health services to approximately 650,000 patients annually and employs about 12,000 individuals.

On August 22, 2013, JHS submitted a breach report to OCR stating that its health information management department had lost paper records containing the PHI of 756 patients in January 2013. JHS's internal investigation determined that an additional three boxes of patient records were also lost in December 2012; however, JHS did not report the additional loss or the increased number of individuals affected to 1,436 until June 7, 2016.

In July 2015, OCR initiated an investigation following a media report that disclosed the PHI of a JHS patient. A reporter had shared a photograph of a JHS operating room screen containing the patient's medical information on social media. JHS subsequently determined that two employees had accessed this patient's electronic medical record without a job-related purpose.

On February 19, 2016, JHS submitted a breach report to OCR reporting that an employee had been selling patient PHI. The employee had inappropriately accessed over 24,000 patients' records since 2011.

OCR's investigation revealed that JHS failed to provide timely and accurate breach notification to the Secretary, conduct enterprise-wide risk analyses, manage identified risks to a reasonable and appropriate level, regularly review information system activity records, and restrict authorization of its workforce members' access to patient ePHI to the minimum necessary to accomplish their job duties.

JHS waived its right to a hearing and did not contest the findings in OCR's Notice of Proposed Determination. Accordingly, OCR issued a Notice of Final Determination and JHS paid the full civil money penalty.

This action occurred in October 2019.

Civil Money Penalty imposed on Texas Health and Human Services Commission

OCR imposed a $1,600,000 civil money penalty against the Texas Health and Human Services Commission (TX HHSC), for violations of the HIPAA Privacy and Security Rules between 2013 and 2017. TX HHSC is part of the Texas HHS system, which operates state supported living centers; provides mental health and substance use services; regulates child care and nursing facilities; and administers hundreds of programs for people who need assistance, including supplemental nutrition benefits and Medicaid. The Department of Aging and Disability Services (DADS), a state agency that administered long-term care services for people who are aging, and for people with intellectual and physical disabilities, was reorganized into TX HHSC in September 2017.

On June 11, 2015, DADS filed a breach report with OCR stating that the ePHI of 6,617 individuals was viewable over the internet, including names, addresses, social security numbers, and treatment information. The breach occurred when an internal application was moved from a private, secure server to a public server and a flaw in the software code allowed access to ePHI without access credentials. OCR's investigation determined that, in addition to the impermissible disclosure, DADS failed to conduct an enterprise-wide risk analysis, and implement access and audit controls on its information systems and applications as required by the HIPAA Security Rule. Because of inadequate audit controls, DADS was unable to determine how many unauthorized persons accessed individuals' ePHI.

TX HHSC waived its right to a hearing and did not contest the findings in OCR's Notice of Proposed Determination. Accordingly, OCR issued a Notice of Final Determination and TX HHSC paid the full civil money penalty.

This action occurred in October 2019.

Resolution Agreement with University of Rochester Medical Center

The University of Rochester Medical Center (URMC) agreed to pay $3 million and take corrective action to settle potential violations of the HIPAA Privacy and Security Rules. URMC includes healthcare components such as the School of Medicine and Dentistry and Strong Memorial Hospital. URMC is one of the largest health systems in New York State with over 26,000 employees.

URMC filed breach reports with OCR in 2013 and 2017 following its discovery that PHI had been impermissibly disclosed through the loss of an unencrypted flash drive and theft of an unencrypted laptop, respectively. OCR's investigation revealed that URMC failed to:

- Conduct an enterprise-wide risk analysis;
- Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level;
- Utilize device and media controls; and
- Employ a mechanism to encrypt and decrypt ePHI when it was reasonable and appropriate to do so.

Of note, in 2010, OCR investigated URMC concerning a similar breach involving a lost unencrypted flash drive and provided technical assistance to URMC. Despite the previous OCR investigation, and URMC's own identification of a lack of encryption as a high risk to ePHI, URMC permitted the continued use of unencrypted mobile devices.

In addition to the monetary settlement, URMC agreed to:

- Conduct an enterprise-wide risk analysis;
- Develop and implement a risk management plan;
- Implement a process for evaluating environmental and operational changes;
- Develop, maintain, review, and revise, if necessary, HIPAA Privacy and Security Rule policies and procedures; and
- Train workforce members on HIPAA Privacy and Security Rule policies and procedures.

This settlement occurred in October 2019.

Resolution Agreement with Sentara Hospitals

Sentara Hospitals (Sentara) agreed to pay $2.175 million and take corrective action to settle potential violations of the HIPAA Privacy and Breach Notification Rules. Sentara is comprised of 12 acute care hospitals with more than 300 sites of care throughout Virginia and North Carolina.

In April 2017, HHS received a complaint alleging that Sentara had sent a bill to an individual containing another patient’s PHI. OCR’s investigation determined that Sentara mailed 577 patients’ PHI to wrong addresses. Sentara reported this incident as a breach affecting 8 individuals because Sentara concluded incorrectly that unless the impermissible disclosure

included patient diagnosis, treatment information, or other medical information, no reportable breach of unsecured PHI had occurred. OCR found that Sentara:

- Failed to report the breach to HHS; and
- Failed to enter into a business associate agreement as required by HIPAA.

In addition to the monetary settlement, Sentara agreed to:

- Develop, maintain, and revise, if necessary, written policies and procedures to comply with the HIPAA Breach Notification Rule.

This settlement occurred in November 2019.

Resolution Agreement with Korunda Medical

Korunda Medical, LLC (Korunda) agreed to pay $85,000 and take corrective action to settle a potential violation of HIPAA's right of access provision of the HIPAA Privacy Rule. Korunda is a Florida-based company that provides comprehensive primary care and interventional pain management to approximately 2,000 patients annually.

In March 2019, OCR received a complaint concerning a Korunda patient alleging that, despite repeated requests, Korunda failed to forward a patient's medical records in electronic format to a third party. OCR provided Korunda with technical assistance on how to correct these matters and closed the complaint. Despite OCR's assistance, Korunda did not provide the requested records, resulting in another complaint to OCR. As a result of OCR's second intervention, the requested records were provided for free in May 2019, and in the format requested. OCR's investigation found that Korunda failed to provide timely access to PHI.

In addition to the monetary settlement, Korunda agreed to:

- Develop right of access policies and procedures to comply with the HIPAA Privacy Rule;
- Train all workforce members on HIPAA's right of access provisions; and
- Submit a listing of all access requests for PHI to OCR every 90 days.

This settlement occurred in December 2019.

Resolution Agreement with West Georgia Ambulance

West Georgia Ambulance, Inc. (West Georgia), agreed to pay $65,000 and take corrective action to settle potential violations of the HIPAA Security Rule. West Georgia is an ambulance company that provides emergency and non-emergency ambulance services in Carroll County, Georgia.

OCR began its investigation after West Georgia filed a breach report in 2013 concerning the loss of an unencrypted laptop containing the PHI of 500 individuals. OCR's investigation uncovered long-standing noncompliance with the HIPAA Rules, including failures to:

- Conduct an accurate and thorough risk analysis of potential risks and vulnerabilities to the confidentiality, integrity, and availability of its ePHI;
- Adopt and implement a security awareness and training program; and
- Implement HIPAA Security Rule policies and procedures.

In addition to the monetary settlement, West Georgia will:

- Conduct an enterprise-wide risk analysis;
- Develop and implement a risk management plan;
- Adopt and implement written policies and procedures to comply with the HIPAA Privacy, Security, and Breach Notification Rules;
- Train workforce members on the revised policies and procedures;
- Identify all business associates and provide copies of business associate agreements to OCR;
- Install HIPAA compliant encryption software on all of its computers; and
- Revise their HIPAA Notice of Privacy Practices.

This settlement occurred in December 2019.