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

For Calendar Year 2020

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

Executive Summary Overview

This report summarizes key HIPAA enforcement activities undertaken by the HHS Office for Civil Rights during the 2020 calendar year. This Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance identifies the number of complaints received and the method by which those complaints were resolved, the number of compliance reviews initiated by OCR and the outcome of each review, the number of audits performed and a summary of findings, the number of subpoenas or inquiries issued, and OCR's anticipated compliance and enforcement initiatives for the following year.

Summary

OCR received 27,182 new complaints alleging violations of the HIPAA Rules and the HITECH Act, representing a decrease of 4% from the number of complaints received in calendar year 2019. OCR resolved 26,530 complaints. Of those, OCR resolved 19,826 (75%) before initiating an investigation. OCR resolved 5,091 (19%) complaints by providing technical assistance in lieu of an investigation (pre-investigational technical assistance). In 872 (54%) of the investigations, a covered entity or business associate took corrective action, and in 80 (5%) of these complaints, OCR provided technical assistance after initiating an investigation (post-investigated technical assistance). OCR resolved 11 complaint investigations with Resolution Agreements/Corrective Action Plans (RA/CAPs), and monetary payments totaling $2,537,500.

OCR completed 566 compliance reviews and required the subject entity to take corrective action or pay a civil money penalty in 86% (485) of these investigations. Eight cases were resolved with RA/CAPs and monetary payments totaling $13,017,400. In the remaining 81 (14%) completed compliance reviews, OCR provided the covered entity or business associate with post-investigated technical assistance (4%), found insufficient evidence of a violation of the HIPAA Rules (9%), or lacked jurisdiction to investigate the allegations (1%). OCR issued four subpoenas, and no audits were initiated.

Recommendations

OCR engaged in numerous outreach activities to increase education to the public and regulated entities and to address compliance deficiencies that have been identified by complaint investigations, compliance reviews, and the audit program. OCR's outreach initiatives and education of the public and the regulated industry included training over 20,000 health care professionals regarding their obligations under the HIPAA right of access standard, launching a HIPAA and COVID-19[1] website to provide consumers and professionals with easy to find information on the COVID-19 related guidance and Notifications of Enforcement Discretion during the pandemic, hosting webinars with ONC to encourage use of the HHS Security Risk Assessment Tool, educating the public on COVID-19 related HIPAA publications, and conducting 28 virtual events for HIPAA covered entities, business associates, and other health care industry stakeholders.

[1] https://www.hhs.gov/hipaa/for-professionals/special-topics/hipaa-covid19/index.html.

Background

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.

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.[2] 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.

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, maintained, or transmitted 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.[3] This report includes information about the Department's enforcement process with regard to the Privacy, Security, and Breach Notification Rules (the HIPAA Rules),

---

[2] 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.

[3] 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 2020.

This report is prepared for the calendar year 2020. 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.

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 to determine if covered entities or business associates are in compliance with the HIPAA Rules. In addition, OCR's compliance activities include conducting audits[4] 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

[4] 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.

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. If OCR determines that it lacks jurisdiction 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 is untimely, OCR closes the case. Where the case is eligible for enforcement, OCR often 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 OCR's attention, such as through the media, referrals from other agencies, 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 CMP 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 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 the imposition of 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 2020 and is currently developing the criteria for implementing future 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 2020, the Department resolved 19 investigations with resolution agreements/CAPs or the imposition of CMPs totaling more than $13.5 million in collections.

As shown in the table below, the number of complaints and breaches reported to OCR continues to increase. Between 2016 and 2020, the number of complaints received by OCR increased 27.13% and the number of compliance reviews initiated by OCR grew by over 94%. During the same period, breaches affecting fewer than 500 individuals increased 14.52% and the number of breaches affecting 500 or more individuals rose 96.41%.

Year	Complaints Received	Compliance Reviews Initiated	Under 500 Breaches Reported	500+ Breaches Reported	% Change in complaints received	% Change in Compliance Reviews Initiated	% Change in Under 500 Breaches Reported	% Change in 500+ Breaches Reported
2020	27,182	746	66,509	656	-3.8% decrease	60.7% increase	6% increase	61% increase
2019	28,261	611	62,771	408	9% increase	36.7% increase	-.5% decrease	35% increase
2018	25,912	447	63,098	302	5.7% increase	-4.7% decrease	4.6% increase	-21.5% decrease
2017	24,506	469	60,322	385	14.6% increase	22% increase	4% increase	15% increase
2016	21,381	384	58,074	334	-	-	-	-

Year	Complaints Received	Compliance Reviews Initiated	Under 500 Breaches Reported	500+ Breaches Reported	% Change in complaints received	% Change in Compliance Reviews Initiated	% Change in Under 500 Breaches Reported	% Change in 500+ Breaches Reported
2016 to 2020	27.13% increase	94.27% increase	14.52% increase	96.41% increase	-	-	-	-

Source: Current and previous Reports to Congress

Enforcement Data

Complaint Resolutions

2020 Complaints

During calendar year 2020, OCR received 27,182 new complaints and carried over 3,203 open complaints from 2019. OCR resolved 26,530 complaints during calendar year 2020.[5] Of those, OCR resolved 19,826 (75%) 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 (2%) or that were untimely (2%). OCR resolved 5,091 complaints (19%) by providing technical assistance in lieu of an investigation.

OCR completed investigations in 1,613 complaints.[6] In 872 of these complaints, OCR required the covered entity or business associate to take corrective action (54% of the complaints investigated); in 80 of these complaints, OCR provided technical assistance after initiating an investigation (5% of the complaints investigated). In 661 of the complaints OCR investigated (41% of the complaints investigated), OCR found insufficient evidence that a violation of the HIPAA Rules had occurred. See Figure 1.

[5] 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.

[6] The number of complaints resolved in a given calendar year is the sum of administrative closures, technical assistance closures and investigated closures.

HHS OFFICE FOR CIVIL RIGHTS

COMPLAINT INVESTIGATIONS AND RESOLUTIONS

NUMBER OF CASES CLOSED AND TYPE OF CLOSURES

JANUARY 1, 2020 THROUGH DECEMBER 31, 2020

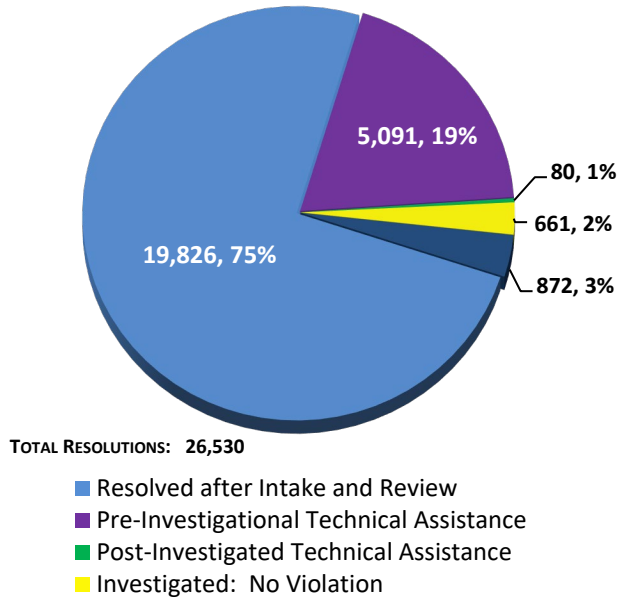

Figure 1

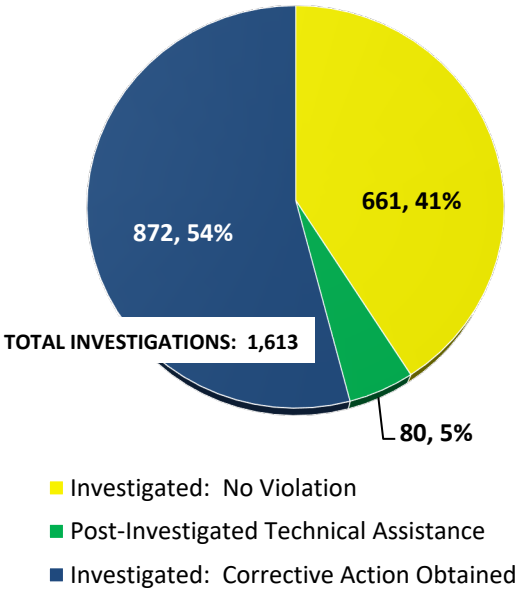

Figure 2

OCR resolved 11 complaint investigations in 2020 through resolution agreements/CAPs and monetary settlements totaling $2,537,500.[7] No complaints were resolved by assessing CMPs.

For the 26,530 complaints OCR resolved in 2020, the top five issues alleged were Impermissible Uses and Disclosures (714 complaints), Safeguards (662 complaints), Right of Access (658 complaints), Administrative Safeguards (Security Rule) (265 complaints), and Technical Safeguards (140 complaints). OCR received 1,079 fewer complaints in 2020 than in 2019, a decrease of four percent (OCR received 28,261 complaints in 2019, compared to 27,182 complaints in 2020).

[7] The 11 complaints that were resolved are Housing Works Community Healthcare, All Inclusive Medical Services, Beth Israel Lahey Health Behavioral Services, Patricia King MD & Associates, Wise Psychiatry, St. Joseph's Hospital and Medical Center, NY Spine Medicine, Riverside Psychiatric Medical Group, Dr. Rajendra Bhayani, University of Cincinnati Medical Center, and Peter Wrobel, MD dba Elite Primary Care. See Appendix for additional information.

Compliance Reviews

2020 Compliance Reviews

During calendar year 2020, OCR initiated 746 compliance reviews to investigate allegations of violations of the HIPAA Rules that did not arise from complaints.[8] Of these, 659 compliance reviews were initiated as a result of a breach report affecting 500 or more individuals and 15 were a result of a breach report affecting fewer than 500 individuals. The remaining 72 compliance reviews were opened based on incidents brought to OCR's attention through multiple complaints regarding an entity or practice, media reports, or other means.

OCR closed 566 compliance reviews in 2020.[9] Of the closed cases, 547 originated from breach reports and 19 originated from other means. The covered entity or business associate took corrective action or paid a CMP in 485 cases (86%). The covered entity or business associate was provided technical assistance after investigation in 22 cases (4%). OCR found that there was insufficient evidence of a violation of the HIPAA Rules in 51 cases (9%). OCR determined that it did not have jurisdiction to investigate the allegations in 8 cases (1%). Of the completed compliance reviews, eight cases were resolved through monetary settlements totaling $13,017,400.[10] See Figure 3.

[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 eight cases that were resolved are Steven A. Porter, MD, Metro Community Health Services dba Agape Health Services, Lifespan, Athens Orthopedic Clinic, CHSPSC, Premera Blue Cross, Aetna Life Insurance Company, and the City of New Haven.

HHS OFFICE FOR CIVIL RIGHTS

COMPLIANCE REVIEWS

NUMBER OF CASES CLOSED WITH TYPES OF CLOSURES

JANUARY 1, 2020 – DECEMBER 31, 2020

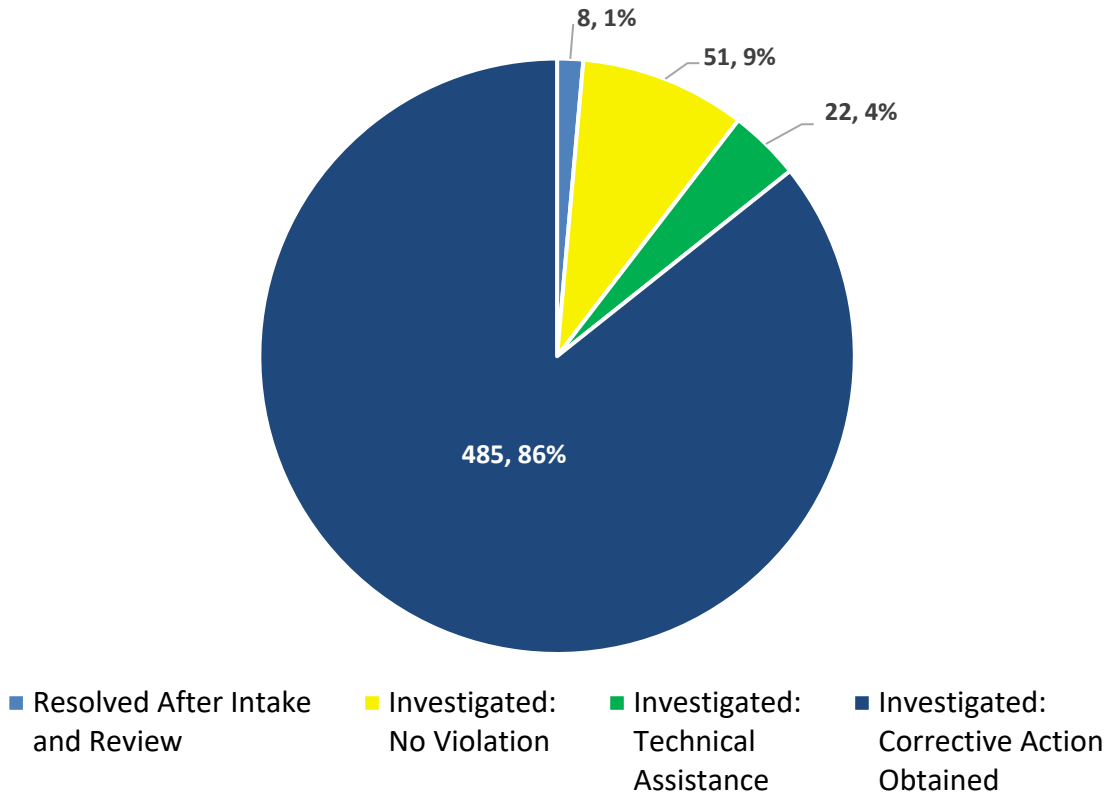

Figure 3

Subpoenas

OCR issued four subpoenas in 2020.

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 individual 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 2020 outreach highlights include:

- In 2020, OCR entered the final year of its contract with Medscape offering on-line provider 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 an individual's right to obtain their health information assists individuals in becoming more involved in their own care. The Medscape module trained 20,987 individuals from January 2020 through September 2020. From July 2017 through September 2020, this module educated a total of 100,927 individuals on the HIPAA Right of Access.
- In response to the COVID-19 public health emergency, OCR launched a HIPAA and COVID-19 website in March 2020 to provide consumers and professionals with easy to find information on the HIPAA Rules during the pandemic. Web content is updated regularly, and OCR works to ensure that guidance and other materials are offered in both English and Spanish. According to Google Analytics, visits to OCR's HIPAA pages increased during the COVID-19 public health emergency from over 300,000 unique visits a month in 2019 to an average of 440,000 unique visits per month during 2020. OCR attributes this increase to the availability of HIPAA and COVID-19 guidance materials, and public interest in this content.
- In April 2020, OCR hosted a webinar for health IT stakeholders on HIPAA privacy and security issues related to COVID-19 and recent OCR actions related to the pandemic. The webinar, available on YouTube, has had over 11,500 views to date. Topics included:
    - COVID-19 and Permissible Disclosures under the HIPAA Privacy Rule
    - Enforcement Discretion and Guidance for Telehealth Remote Communications
    - Guidance for Disclosures to First Responders and Public Health Authorities
    - Enforcement Discretion for Business Associates to Use and Disclose PHI for Public Health and Health Oversight Activities
    - Enforcement Discretion for Community-Based Testing Sites
- Despite the COVID-19 public health emergency, OCR's outreach efforts continued on-pace with 28 virtual events for HIPAA covered entities, business associates, and other health care industry stakeholders. Many of these virtual conferences focused specifically on OCR actions related to the pandemic, including HIPAA enforcement discretion and guidance for telehealth.
- In 2020, OCR and ONC hosted a series of webinars to review updates to the popular HHS Security Risk Assessment (SRA) Tool, highlighting a number of enhancements which make the tool 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. In 2020, OCR and ONC held five webinars to illustrate and promote the tool's use.

Audits

OCR did not initiate any audits in 2020. OCR released its 2016-2017 HIPAA Audits Industry Report that reviewed selected healthcare entities and business associates for compliance with certain provisions of the HIPAA Rules. The audit results found that covered entities generally are compliant with the timeliness requirements for providing breach notification to individuals and prominently posting a Notice of Privacy Practices on their website, but covered entities and business associates generally were not compliant with requirements to have all of the required content for a breach notification and Notice of Privacy Practices and implement the Security Rule's requirements for a risk analysis and risk management. These results were consistent with OCR's findings within its enforcement program involving complaint and compliance review investigations. The audits generally did not provide OCR with any new information about the regulated industry's compliance with the HIPAA Rules.

Appendix

Resolution Agreements[11] in 2020

Resolution Agreement with Steven A. Porter, M.D.

Steven A. Porter, M.D. (Porter), agreed to pay $100,000 and take corrective action to settle potential violations of the HIPAA Security Rule. Dr. Porter's medical practice, based in Ogden, Utah, provides gastroenterological medical services.

OCR began investigating Porter after it filed a breach report related to a dispute with a business associate. OCR's investigation determined that Porter had never conducted a risk analysis at the time it filed the breach report, and despite significant technical assistance throughout the investigation, had failed to complete an accurate and thorough risk analysis after the breach and failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

In addition to the monetary settlement, Porter agreed to:

- Complete an enterprise-wide risk analysis;
- Develop comprehensive policies and procedures to comply with the HIPAA Rules; and
- Train all workforce members who use or disclose PHI on revised policies and procedures.

This settlement occurred in February 2020. The resolution agreement is available at the following link: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/porter/index.html.

Resolution Agreement with Metropolitan Community Health Services dba Agape Health Services

Metropolitan Community Health Services doing business as Agape Health Services (Agape) agreed to pay $25,000 and take corrective action to settle potential violations of the HIPAA Security Rule. Agape is a Federally Qualified Health Center that provides a variety of discounted health services to the underserved population in rural North Carolina.

On June 9, 2011, Agape filed a breach report with OCR following discovery that a misdirected email transmission resulted in the compromise of the ePHI of 1,263 individuals. OCR's investigation revealed longstanding, systemic noncompliance with the HIPAA Security Rule. Specifically, Agape failed to conduct any risk analyses, implement any HIPAA Security Rule

[11] 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 2020. No CMPs were assessed in 2020.

policies and procedures, and provide workforce members with security awareness training until 2016.

In addition to the monetary settlement, Agape agreed to:

- Complete an enterprise-wide risk analysis;
- Develop and implement risk management;
- Review and revise written policy and procedures to comply with the HIPAA Rules; and
- Train workforce members on revised policies and procedures.

This settlement occurred in March 2020. The resolution agreement is available at the following link: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/metro/index.html.

Resolution Agreement with CHSPSC

CHSPSC, LLC agreed to pay $2,300,000 and adopt a corrective action plan to settle potential violations of the HIPAA Privacy and Security Rules. CHSPSC provides a variety of business associate services, including IT and health information management, to hospitals and physician clinics indirectly owned by Community Health Systems, Inc., in Tennessee.

In April 2014, the Federal Bureau of Investigation notified CHSPSC that it had traced a hacking group's advanced persistent threat to CHSPSC's information system. Despite this notice, the hackers continued to access and exfiltrate the ePHI of over 6.1 million individuals until August 2014. The hackers used compromised administrative credentials to remotely access CHSPSC's information system through its virtual private network.

OCR's investigation found longstanding, systemic noncompliance with the HIPAA Security Rule, including failure to conduct a risk analysis, and failure to implement information system activity review, security incident procedures, and access controls.

In addition to the monetary settlement, CHSPSC agreed to:

- Conduct an enterprise-wide risk analysis;
- Develop and implement risk management;
- Revise its written policies and procedures to comply with the HIPAA Security Rule; and
- Train workforce members on revised HIPAA Security Rule policies and procedures.

This settlement occurred in March 2020. The resolution agreement is available at the following link: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/chspsc/index.html.

Resolution Agreement with Premera Blue Cross

Premera Blue Cross (PBC) agreed to pay $6.85 million and implement a corrective action plan to settle potential violations of the HIPAA Privacy and Security Rules. PBC operates in Washington and Alaska, and is the largest health plan in the Pacific Northwest, serving more than two million people.

On March 17, 2015, PBC filed a breach report on behalf of itself and its network of affiliates stating that cyber-attackers had hacked into its information technology system. The hackers used a phishing email to install malware that gave them access to PBC's IT system in May 2014, which went undetected for nearly nine months. This undetected attack resulted in the disclosure of more than 10.4 million individuals' ePHI, including names, addresses, dates of birth, email addresses, Social Security numbers, financial information, and health plan clinical information.

OCR's investigation found systemic noncompliance with the HIPAA Rules, including failure to conduct an enterprise-wide risk analysis, and failure to implement risk management and audit controls.

In addition to the monetary settlement, PBC agreed to:

- Conduct an enterprise-wide risk analysis;
- Develop and implement risk management; and
- Adopt and implement written policies and procedures to comply with the HIPAA Security Rule.

This settlement occurred in March 2020. The resolution agreement is available at the following link: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/premera/index.html.

Resolution Agreement with Lifespan Health System Affiliated Covered Entity

Lifespan Health System Affiliated Covered Entity (Lifespan) agreed to pay $1,040,000 and take corrective action to settle potential violations of the HIPAA Privacy and Security Rules related to the theft of an unencrypted laptop. Lifespan is a non-profit health system based in Rhode Island.

OCR initiated its investigation after Lifespan filed a breach report on April 21, 2017, regarding the theft of an affiliated hospital employee's laptop containing ePHI that included the names, medical record numbers, demographic information, and medication information of 20,431 individuals. OCR's investigation determined that there was systemic noncompliance with the HIPAA Rules, including a failure to encrypt ePHI on laptops after Lifespan determined it was reasonable and appropriate to do so. OCR also uncovered a lack of device and media controls, and a failure to have a business associate agreement in place with the Lifespan.

In addition to the monetary settlement, Lifespan agreed to:

- Develop policies and procedures to comply with the HIPAA Privacy and Security Rules;
- Provide written reporting to OCR pertaining to the encryption of devices that contain ePHI and have access to its network;

- Complete an accounting of business associate agreements between Lifespan and its affiliated healthcare providers; and
- Train all workforce members who have access to ePHI on its new policies and procedures.

This settlement occurred in June 2020. The resolution agreement is available at the following link: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/lifespan/index.html.

Resolution Agreement with Housing Works Community Healthcare

Housing Works Community Healthcare (HWCH) agreed to pay $38,000 and take corrective action to settle a potential violation of the right of access provision of the HIPAA Privacy Rule. HWCH is a New York City based not-for-profit organization that receives HHS funding under the Federal 330 Health Center Program. The organization provides healthcare, advocacy, homeless services, job training, reentry services, and legal aid support for people living with and affected by HIV/AIDS.

In July 2019, OCR received a complaint alleging that, in June 2019, HWCH failed to provide the complainant with a copy of his medical records. OCR provided HWCH with technical assistance on the HIPAA right of access requirements and closed the complaint. On August 13, 2019, OCR received a second complaint alleging that HWCH still had not provided the complainant with a copy of his medical records. OCR initiated an investigation, and, as a result of OCR's intervention, the requested records were provided to the complainant. OCR's investigation found that HWCH failed to provide timely access to PHI.

In addition to the monetary settlement, HWCH 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 while under the terms of the corrective action plan.

This settlement occurred in June 2020. The resolution agreement is available at the following link: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/right-of-access-initiative/index.html.

Resolution Agreement with All Inclusive Medical Services

All Inclusive Medical Services, Inc. (AIMS) agreed to pay $15,000 and take corrective action to settle a potential violation of the HIPAA Privacy Rule's right of access provision. AIMS, based in Carmichael, California, is a multi-specialty family medicine clinic that provides a variety of services, including internal medicine and pain management and rehabilitation.

OCR received a complaint alleging that AIMS refused to give a patient access to her medical records when it denied her requests to inspect and receive a copy of her records. OCR initiated an investigation and determined that AIMS's actions were potential violations of the HIPAA right of access standard. As a result of OCR's investigation, AIMS sent the patient her medical records. The HIPAA Privacy Rule generally requires covered health care providers to provide medical records within 30 days of the request at a reasonable cost-based fee.

In addition to the monetary settlement, AIMS agreed to:

- Develop right of access policies and procedures to comply with the HIPAA Privacy Rule; and
- Train all workforce members who have access to PHI on the revised policies and procedures.

This settlement occurred in July 2020. The resolution agreement is available at the following link: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/right-of-access-initiative/index.html.

Resolution Agreement with Athens Orthopedic Clinic

Athens Orthopedic Clinic PA (Athens Orthopedic) agreed to pay $1,500,000 and adopt a corrective action plan to settle potential violations of the HIPAA Privacy and Security Rules. Athens Orthopedic is located in Georgia and provides orthopedic services to the local community.

On June 26, 2016, a journalist notified Athens Orthopedic that a database of their patient records may have been posted online for sale. A hacker subsequently contacted Athens Orthopedic and demanded money in return for a complete copy of the database it stole. Athens Orthopedic determined that the hacker used a vendor's credentials to access its electronic medical record system and exfiltrate patient health data. The hacker continued to access ePHI for over a month.

On July 29, 2016, Athens Orthopedic filed a breach report informing OCR that 208,557 individuals were affected by this breach, and that the ePHI disclosed included names, dates of birth, Social Security numbers, medical procedures, test results, and health insurance information.

OCR's investigation discovered longstanding, systemic 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.

In addition to the monetary settlement, Athens Orthopedic agreed to:

- Conduct an enterprise-wide risk analysis;
- Develop and implement risk management;
- Adopt and implement written policies and procedures to comply with the HIPAA Privacy and Security Rules;
- Train workforce members on HIPAA Privacy and Security Rule policies and procedures; and
- Identify all business associates and provide copies of business associate agreements.

This settlement occurred in July 2020. The resolution agreement is available at the following link: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/athens-orthopedic/index.html.

Resolution Agreement with Beth Israel Lahey Health Behavioral Services

Beth Israel Lahey Health Behavioral Services (BILHBS) agreed to pay $70,000 and adopt a corrective action plan to settle a potential violation of the HIPAA Privacy Rule's right of access provision. BILHBS is the largest network of mental health and substance use disorder services in eastern Massachusetts.

In April 2019, OCR received a complaint alleging that BILHBS failed to respond to a request from a personal representative seeking access to her father's medical records. OCR initiated an investigation and determined that BILHBS' failure to provide the requested medical records was a potential violation of the HIPAA right of access standard. As a result of OCR's investigation, BILHBS sent the personal representative the requested medical records in October 2019.

In addition to the monetary settlement, BILHBS agreed to:

- Develop right of access policies and procedures to comply with the HIPAA Privacy Rule; and
- Train all workforce members on revised policies and procedures.

This settlement occurred in August 2020. The resolution agreement is available at the following link: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/right-of-access-initiative/index.html.

Resolution Agreement with Patricia King MD & Associates

Patricia King MD & Associates (King MD) agreed to pay $3,500 and adopt a corrective action plan to settle a potential violation of the HIPAA Privacy Rule's right of access provision. King MD is a small health care provider of psychiatric services in Virginia.

In October 2018, OCR received a complaint alleging that King MD failed to respond to an individual's request for access to her medical records. OCR provided King MD with technical assistance on the HIPAA right of access requirements and closed the complaint. In February 2019, OCR received a second complaint alleging that the practice still had not provided the individual with access to her medical records. OCR initiated an investigation and determined that the practice's failure to provide the requested medical records was a potential violation of the HIPAA right of access standard. As a result of OCR's investigation, King MD sent the individual her medical records in July 2020.

In addition to the monetary settlement, King MD agreed to:

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

This settlement occurred in August 2020. The resolution agreement is available at the following link: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/right-of-access-initiative/index.html.

Resolution Agreement with Wise Psychiatry

Wise Psychiatry, PC (Wise Psychiatry) agreed to pay $10,000 and adopt a corrective action plan to settle a potential violation of the HIPAA Privacy Rule's right of access provision. Wise Psychiatry is a small health care provider that provides psychiatric services in Colorado.
In February 2018, OCR received a complaint alleging that Wise Psychiatry failed to provide a personal representative with access to his minor son's medical records. OCR provided Wise Psychiatry with technical assistance on the HIPAA right of access requirements and closed that complaint. In October 2018, OCR received a second complaint alleging that Wise Psychiatry still had not provided the personal representative with access to his minor son's medical records. OCR initiated an investigation and determined that Wise Psychiatry's failure to provide the requested medical records was a potential violation of the HIPAA right of access standard. As a result of OCR's investigation, Wise Psychiatry sent the personal representative his son's medical record.

In addition to the monetary settlement, Wise Psychiatry agreed to:

- Distribute its recently developed policies and procedures to all workforce members; and
- Train all workforce members on its right of access policies and procedures.

This settlement occurred in August 2020. The resolution agreement is available at the following link: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/right-of-access-initiative/index.html.

Resolution Agreement with St. Joseph's Hospital and Medical Center

Dignity Health, doing business as St. Joseph's Hospital and Medical Center (SJHMC), agreed to take corrective actions and pay $160,000 to settle a potential violation of the HIPAA Privacy Rule's right of access provision. SJHMC, based in Phoenix, Arizona, is a large, acute care hospital with several hospital-based clinics that provides a wide range of health, social, and support services.

On April 25, 2018, OCR received a complaint from a mother alleging that beginning in January 2018, she made multiple requests to SJHMC for a copy of her son's medical records, as his personal representative. SJHMC provided some of the requested records, but despite the mother's follow up requests in March, April, and May 2018, SJHMC did not provide all of the requested records. OCR initiated an investigation and determined that SJHMC's actions were a potential violation of the HIPAA right of access standard. As a result of OCR's investigation, SJHMC sent all of the requested medical records to the mother on December 19, 2019, more than 22 months after her initial request.

In addition to the monetary settlement, SJHMC agreed to:

- Develop right of access policies and procedures to comply with the HIPAA Privacy Rule;
- Train workforce members on HIPAA's right of access provisions; and
- Submit a listing of all business associates involved in HIPAA right of access requests and copies of associated business associate agreements to OCR.

This settlement occurred in September 2020. The resolution agreement is available at the following link: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/sjhmc/index.html.

Resolution Agreement with NY Spine Medicine

NY Spine Medicine (NY Spine) agreed to take corrective actions and pay $100,000 to settle a potential violation of the HIPAA Privacy Rule's right of access standard. NY Spine is a private medical practice specializing in neurology and pain management with offices in New York, NY, and Miami Beach, FL.

In July 2019, OCR received a complaint from an individual alleging that beginning in June 2019, she made multiple requests to NY Spine for a copy of her medical records. NY Spine provided some of the records, but did not provide the diagnostic films that the individual specifically requested. OCR initiated an investigation and determined that NY Spine's failure to provide timely access to all of the requested medical records was a potential violation of the right of

access standard. As a result of OCR's investigation, the complainant subsequently received all of the requested medical records.

In addition to the monetary settlement, NY Spine agreed to:

- Develop right of access policies and procedures to comply with the HIPAA Privacy Rule; and
- Train all workforce members on HIPAA's right of access provisions.

This settlement occurred in September 2020. The resolution agreement is available at the following link: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/nyspine/index.html.

Resolution Agreement with Aetna Life Insurance Company

Aetna Life Insurance Company and the affiliated covered entity (Aetna) agreed to pay $1,000,000 and adopt a corrective action plan to settle potential violations of the HIPAA Privacy and Security Rules. Aetna is an American managed health care company that sells traditional and consumer-directed health insurance and related services.

In June 2017, Aetna submitted a breach report to OCR stating that on April 27, 2017, Aetna discovered that two web services used to display plan-related documents to health plan members allowed documents to be accessible and subsequently indexed by various internet search engines. Aetna reported that 5,002 individuals were affected by this breach, and the PHI disclosed included names, insurance identification numbers, claim payment amounts, procedure service codes, and dates of service.

In August 2017, Aetna submitted another breach report to OCR stating that on July 28, 2017, benefit notices were mailed to members using window envelopes which exposed individuals' PHI. Aetna reported that 11,887 individuals were affected by this impermissible disclosure.

In November 2017, Aetna submitted another breach report to OCR stating that on September 25, 2017, a research study mailing sent to Aetna plan members exposed individuals' PHI. Aetna reported that 1,600 individuals were affected by this impermissible disclosure.

OCR's investigation revealed that, in addition to the impermissible disclosures, Aetna failed to perform periodic technical and nontechnical evaluations of operational changes affecting the security of their ePHI; implement procedures to verify the identity of persons or entities seeking access to ePHI; limit PHI disclosures to the minimum necessary to accomplish the purpose of the use or disclosure; and have in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI.

In addition to the monetary settlement, Aetna agreed to:

- Adopt and implement written policies and procedures to comply with the HIPAA Privacy and Security Rules; and
- Train all workforce members who have access to PHI on revised policies and procedures.

This settlement occurred in October 2020. The resolution agreement is available at the following link: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/aetna/index.html.

Resolution Agreement with City of New Haven

The City of New Haven, Connecticut (New Haven) agreed to pay $202,400 and implement a corrective action plan to settle potential violations of the HIPAA Privacy and Security Rules. The New Haven Health Department (NHHD), among other activities, operates a public health clinic that provides preventative medical services, including adult and pediatric immunizations.

In January 2017, NHHD filed a breach report with OCR stating that a former employee may have accessed a file on a New Haven computer containing the PHI of 498 individuals. OCR's investigation revealed that, on July 27, 2016, a former employee returned to NHHD, eight days after being terminated, logged into her old computer with her still-active user name and password, and downloaded PHI that included names, addresses, dates of birth, race/ethnicity, gender, and sexually transmitted disease test results onto a USB drive. Additionally, OCR found that the former employee had shared her user ID and password with an intern, who continued to use these login credentials to access PHI on NHHD's network after the employee was terminated.

OCR's investigation determined that NHHD failed to conduct an enterprise-wide risk analysis, and failed to implement termination procedures, access controls such as unique user identification, and HIPAA Privacy Rule policies and procedures.

In addition to the monetary settlement, New Haven agreed to:

- Conduct an enterprise-wide risk analysis;
- Develop and implement risk management;
- Adopt and implement written policies and procedures to comply with the HIPAA Privacy and Security Rules; and
- Train workforce members on HIPAA Privacy and Security Rule policies and procedures.

This settlement occurred in October 2020. The resolution agreement is available at the following link: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/new-haven/index.html.

Resolution Agreement with Riverside Psychiatric Medical Group

Riverside Psychiatric Medical Group (RPMG) agreed to take corrective actions and pay $25,000 to settle a potential violation of the HIPAA Privacy Rule's right of access standard. RPMG,

based in Riverside, California, is a group practice specializing in child and adolescent psychiatry, geriatric psychiatry, neuropsychiatry, psychology, and substance use disorders.

In March 2019, OCR received a complaint from a patient alleging that RPMG failed to provide her with a copy of her medical records despite multiple requests to RPMG beginning in February 2019. Shortly after receiving the complaint, OCR provided RPMG with technical assistance on how to comply with the HIPAA right of access requirements and closed the matter. In April 2019, however, OCR received a second complaint alleging that RPMG still had not provided the complainant with access to her medical records.

OCR initiated an investigation and determined that RPMG's failure to take action in response to the individual's request was a potential violation of the HIPAA right of access standard. RPMG claimed that because the requested records included psychotherapy notes, they did not have to comply with the access request. While the HIPAA Rules do not require production of psychotherapy notes, they do require covered entities (1) to provide requestors a written explanation when it denies any records request in whole or in part (which RPMG did not do), and (2) to provide the individual access to his or her medical records other than psychotherapy notes (and information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding).

As a result of OCR's investigation, RPMG sent the individual all the requested information in her medical record, excluding psychotherapy notes, in October 2020.

In addition to the monetary settlement, RPMG agreed to:

- Revise its right of access policies and procedures to comply with the HIPAA Privacy Rule;
- Train workforce members on HIPAA's right of access provisions; and
- Submit a listing of all access requests for PHI to OCR every 90 days while under the terms of the corrective action plan.

This settlement occurred in October 2020. The resolution agreement is available at the following link: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/riverside/index.html.

Resolution Agreement with Dr. Rajendra Bhayani

Dr. Rajendra Bhayani, a private practitioner specializing in otolaryngology in Regal Park, New York, agreed to take corrective actions and pay $15,000 to settle a potential violation of the HIPAA Privacy Rule's right of access standard.

In September 2018, OCR received a complaint alleging that Dr. Bhayani failed to provide a patient with access to her medical records following her request in July 2018. OCR responded by providing Dr. Bhayani with technical assistance on complying with HIPAA's right of access requirements and closed the complaint. In July 2019, however, OCR received a second complaint alleging that Dr. Bhayani still had not provided the complainant with access to her records. OCR determined that Dr. Bhayani's failure to provide the requested medical records

was a potential violation of the HIPAA right of access standard. As a result of OCR's investigation, the complainant received a complete copy of her medical records in September 2020.

In addition to the monetary settlement, Dr. Bhayani agreed to:

- Revise his right of access policies and procedures to comply with the HIPAA Privacy Rule;
- Train workforce members on HIPAA's right of access provisions; and
- Submit a listing of all access requests for PHI to OCR every 90 days while under the terms of the corrective action plan.

This agreement occurred in October 2020. The resolution agreement is available at the following link: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/bhayani/index.html.

Resolution Agreement with the University of Cincinnati Medical Center

The University of Cincinnati Medical Center, LLC (UCMC), an academic medical center providing healthcare services to the Greater Cincinnati community, agreed to take corrective actions and pay $65,000 to settle a potential violation of the HIPAA Privacy Rule's right of access standard.

In May 2019, OCR received a complaint alleging that UCMC failed to respond to a patient's February 22, 2019, records access request directing UCMC to send an electronic copy of her medical records maintained in UCMC's electronic health record (EHR) to her lawyers. OCR initiated an investigation and determined that UCMC failed to timely provide a copy of the requested medical records in potential violation of the HIPAA Privacy Rule, which includes the right of patients to have electronic copies of records in an EHR transmitted directly to a third party. As a result of OCR's investigation and intervention, the complainant received all of the requested medical records in August 2019.

In addition to the monetary settlement, UCMC agreed to:

- Develop right of access policies and procedures to comply with the HIPAA Privacy Rule;
- Train workforce members on HIPAA's right of access provisions; and
- Submit a listing of all business associates involved in HIPAA right of access requests and copies of associated business associate agreements to OCR.

This agreement occurred in November 2020. The resolution agreement is available at the following link: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/ucmc/index.html.

Resolution Agreement with Peter Wrobel, MD dba Elite Primary Care

Peter Wrobel, M.D., P.C., doing business as Elite Primary Care (Elite) agreed to take corrective actions and pay $36,000 to settle a potential violation of the HIPAA Privacy Rule's right of access standard. Elite provides primary care health services in Georgia.

In April 2019, OCR received a complaint alleging that Elite failed to respond to a patient's request for access to his medical records. In May 2019, OCR provided technical assistance to Elite on the HIPAA right of access requirements and closed the complaint. In October 2019, OCR received a second complaint alleging that Elite still had not provided the patient with access to his medical records. OCR initiated an investigation and determined that Elite's failure to provide the requested medical records was a potential violation of the HIPAA right of access standard. As a result of OCR's investigation, the patient received a copy of his medical record in May 2020.

In addition to the monetary settlement, Elite agreed to:

- Revise its right of access policies and procedures to comply with the HIPAA Privacy Rule; and
- Train all workforce members on HIPAA's right of access provisions.

This agreement occurred in December 2020. The resolution agreement is available at the following link: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/elite-primary-care/index.html.