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

For Calendar Year 2021

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 Health Insurance Portability and Accountability Act of 1996 (HIPAA) enforcement activities undertaken by the HHS Office for Civil Rights (OCR) during the 2021 calendar year. The HITECH Act requires OCR to produce an Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance that identifies the number of complaints received, the method by which those complaints were resolved, the number of compliance reviews initiated by OCR, the outcome of each review, the number of audits performed, a summary of audit findings, the number of subpoenas or inquiries issued, and OCR's anticipated compliance and enforcement initiatives for the following year. OCR did not perform any audits in 2021 due to a lack of financial resources.

There have been significant increases in HIPAA complaints received (39% increase from 2017 to 2021) and large breaches reported (58% increase from 2017 to 2021), without any increases in appropriations during that same time period. Further, in April 2019, as a part of HHS's review of existing regulations, HHS issued a Notification of Enforcement Discretion Regarding HIPAA Civil Money Penalties that significantly reduced the maximum annual cap for three of the four penalty tiers. HHS determined that this change reflected the better reading of the HITECH Act.[1] OCR requested that the HITECH civil monetary penalty caps be increased in the HHS FY 2023 Discretionary A-19 Legislative Supplement that was sent to Congress in September 2021. These factors have combined to cause a severe strain on OCR's limited staff and resources. This lack of necessary funding limits OCR's HIPAA enforcement activities during a time of substantial growth in cybersecurity attacks to the health care sector.

Summary

OCR received 34,077 new complaints alleging violations of the HIPAA Rules and the HITECH Act, representing an increase of 25% from the number of complaints received in calendar year 2020. OCR resolved 26,420 complaints. Of those, OCR resolved 20,661 (78%) before initiating an investigation. OCR resolved 4,139 (16%) complaints by providing technical assistance in lieu of an investigation (pre-investigational technical assistance). In 714 (3%) of the investigations, a covered entity or business associate took corrective action, and in 89 (<1%) of these complaints, OCR provided technical assistance after initiating an investigation (post-investigated technical assistance). OCR resolved 13 complaint investigations with Resolution Agreements and Corrective Action Plans (RA/CAPs) and monetary settlements totaling $815,150, and two complaint investigations with civil money penalties totaling $150,000.

OCR completed 573 compliance reviews and required subject entities to take corrective action or pay a civil money penalty in 83% (475) of these investigations. Two compliance reviews were resolved with RA/CAPs and monetary payments totaling $5,125,000. In the remaining 98 (17%) completed compliance reviews, OCR provided the covered entity or business associate with post-investigation technical assistance (3%), found insufficient evidence of a violation of the HIPAA Rules (11%), or lacked jurisdiction to investigate the allegations (3%). OCR issued one subpoena, and no audits were initiated.

OCR engaged in numerous outreach activities to increase education to the public and regulated

[1] www.federalregister.gov/documents/2019/04/30/2019-08530/notification-of-enforcement-discretion-regarding-hipaa-civil-money-penalties.

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 conducting 218 outreach events to the healthcare community with a focus on pandemic initiatives, including HIPAA enforcement discretion and providing guidance on telehealth.

OCR's web content is updated regularly, providing information and guidance in both English and Spanish. Visits to OCR's HIPAA pages increased during the COVID-19 public health emergency, including OCR's HIPAA and COVID-19 webpage[2] that provides consumers and professionals with easy to find information on all of OCR's COVID-19 related announcements, bulletins, guidance, and Notifications of Enforcement Discretion, and averaged over 450,000 unique visits per month during 2021.

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;

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

- 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.[3] 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.[4] This report includes information about the Department's enforcement process with regard to the Privacy, Security, and Breach Notification Rules (the HIPAA Rules),

---

[3] 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.

[4] A separate Report to Congress, available at 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 2021.

This report is prepared for the calendar year 2021. The Reports to Congress on Compliance with the HIPAA Privacy and Security Rules for previous years are available at 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[5] 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 act only on complaints that meet the following conditions[6]:

- 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.

[5] 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.
[6] *See also* 45 C.F.R. §160.306(c) (1) and (2) which provide that a complaint will be investigated when a preliminary review of the facts indicates a possible violation due to willful neglect, and any other complaint may be investigated.

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

The HIPAA regulations provide that the Secretary may initiate a compliance review into the practices of an entity subject to HIPAA in circumstances other than in response to a complaint.[7] OCR may open compliance review investigations 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 multiple complaints alleging the same or similar violations against the same entity.

If individual complaints are received during the course of an open investigation that assert the same allegations/potential violations being investigated in the open transaction, OCR will consolidate the complaint(s) into the open investigation (*e.g.* a compliance review or an investigation of a reported breach).[8] Multiple complaints alleging the same or similar violations demonstrate systemic compliance deficiencies that are better investigated under one transaction rather than on an individual complaint basis for purposes of achieving compliance.

OCR may also initiate a compliance review investigation if information gathered from an ongoing investigation requires such action. For example, while investigating a breach reported by a covered entity, OCR may learn that the breach was caused by the covered entity's business associate and may therefore open a compliance review of the business associate.

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.

---

[7] "The Department generally conducts compliance reviews to investigate allegations of violations of the HIPAA Rules brought to the Department's attention through a mechanism other than a complaint." (2013 Omnibus Rule, Page 5579) *See also* 45 C.F.R. §160.308(a) and (b) which provide that compliance reviews will be conducted when a preliminary review of the facts indicates a possible violation due to willful neglect, and compliance reviews may be conducted to determine compliance in any other circumstances.

[8] When a complaint is consolidated into an open investigation, it is not counted as closed since it would mean double counting (*i.e.,* counting it closed and consolidated). The consolidated complaint is deleted and not counted as closed so as not to double-count complaint cases.

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 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 ageneral 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 impose 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 the 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 2021 and is currently developing the criteria for implementing future audits.

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 in 2021, OCR resolved 17 investigations with resolution agreements/CAPs or the imposition of CMPs totaling $6.1 million in collections.

As shown in the table below, the number of complaints and breaches reported to OCR continues to increase. Between 2017 and 2021, the number of complaints received by OCR increased 39% and the number of compliance reviews initiated by OCR grew by 44%. During the same period, breaches affecting fewer than 500 individuals increased 5% and the number of breaches affecting 500 or more individuals rose 58%.

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
2021	34,077	674	63,571	609	25% increase	-10% decrease	-4% decrease	-7% decrease

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	-4% decrease	22% increase	6% increase	61% increase
2019	28,261	611	62,771	408	9% increase	37% increase	-.5% decrease	35% increase
2018	25,912	447	63,098	302	6% increase	-5% decrease	5% increase	-22% decrease
2017	24,506	469	60,322	385	-	-	-	-
2017 to 2021	-	-	-	-	39% increase	44% increase	5% increase	58% increase

Source: Current and previous Reports to Congress

Enforcement Data

Complaint Resolutions

2021 Complaints

During calendar year 2021, OCR received 34,077 new complaints and carried over 3,814 open complaints from 2020. OCR resolved 26,420 complaints during calendar year 2021.[9] Of those, OCR resolved 20,661 (78%) 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 (3%) or that were untimely (1%). OCR resolved 4,139 complaints (16%) by providing technical assistance in lieu of an investigation. See Figure 1.

[9] The number of 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.

OCR completed investigations in 1,620 complaints.[10] In 714 of these complaints, OCR required the covered entity or business associate to take corrective action (44% of the complaints investigated). In 89 of these complaints, OCR provided technical assistance after initiating an investigation (5% of the complaints investigated). In 817 of the complaints OCR investigated (50% of the complaints investigated), OCR found insufficient evidence that a violation of the HIPAA Rules had occurred. See Figure 2.

HHS OFFICE FOR CIVIL RIGHTS

COMPLAINT INVESTIGATIONS AND RESOLUTIONS

NUMBER OF CASES CLOSED AND TYPE OF CLOSURES

JANUARY 1, 2021 THROUGH DECEMBER 31, 2021

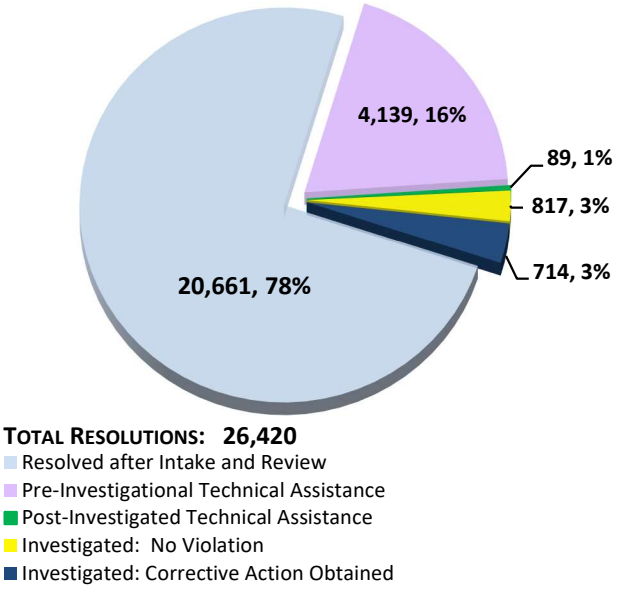

Figure 1

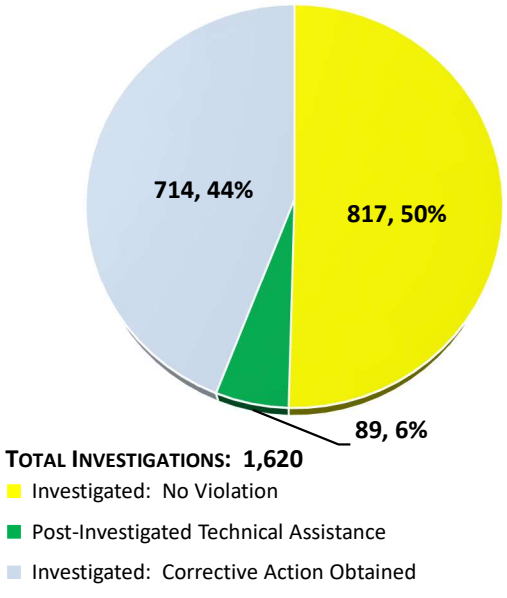

Figure 2

OCR resolved 13 complaint investigations in 2021 through resolution agreements and/or CAPs and monetary settlements totaling $815,150.[11] Two complaints were resolved by assessing CMPs in the amount of $150,000.

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

[11] The 13 complaint investigations are: Banner Health, Renown Health, Sharp Healthcare dba Sharp Rees-Stealy Medical Centers, The Arbour dba Arbour Hospital, Village Plastic Surgery, The Diabetes, Endocrinology & Lipidology Center, Children's Hospital & Medical Center, Wake Health Medical Group, Denver Retina Center, Rainrock Treatment Center dba Monte Nido Rainrock, Advanced Spine & Pain, Dr. Jacob and Associates, and Dr. Donald Brockley, D.D.M.

For the 26,420 complaints OCR resolved in 2021, the top five issues alleged were Impermissible Uses and Disclosures (702 complaints), Right of Access (667 complaints), Safeguards (637 complaints), Administrative Safeguards (Security Rule) (156 complaints), and Breach-Notice to Individuals (97 complaints). OCR received 6,895 more complaints in 2021 than in 2020, an increase of 25 percent (OCR received 27,182 complaints in 2020, compared to 34,077 complaints in 2021).

Compliance Reviews

2021 Compliance Reviews

During calendar year 2021, OCR initiated 674 compliance reviews to investigate allegations of violations of the HIPAA Rules that did not arise from complaints.[12] Of these, 609 compliance reviews were initiated as a result of a breach report affecting 500 or more individuals and 22 were a result of a breach report affecting fewer than 500 individuals. The remaining 43 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 573 compliance reviews in 2021, the vast majority of these cases were resolved following an investigation with the regulated entity taking corrective actions due to OCR involvement during the course of the investigation to come into compliance, agreeing to a settlement with a corrective action plan, or the imposition of a CMP.[13] Of the closed cases, 554 originated from breach reports and 19 originated from other means. The covered entity or business associate took corrective action or paid a CMP in 475 cases (83%). The covered entity or business associate was provided technical assistance after investigation in 16 cases (3%). OCR found that there was insufficient evidence of a violation of the HIPAA Rules in 66 cases (11%), and OCR determined that it did not have jurisdiction to investigate the allegations in 16 cases (3%). Of the completed compliance reviews, two cases were resolved with resolution agreements, CAPs and monetary settlements totaling $5,125,000.[14] See Figure 3.

[12] 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.

[13] 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.

[14] The two cases that were resolved with resolution agreements, corrective action plans and monetary settlements are Excellus Health Plan and Peachstate Health Management dba AEON Clinical Laboratories.

HHS OFFICE FOR CIVIL RIGHTS

COMPLIANCE REVIEWS

NUMBER OF CASES CLOSED AND TYPES OF CLOSURES

JANUARY 1, 2021 – DECEMBER 31, 2021

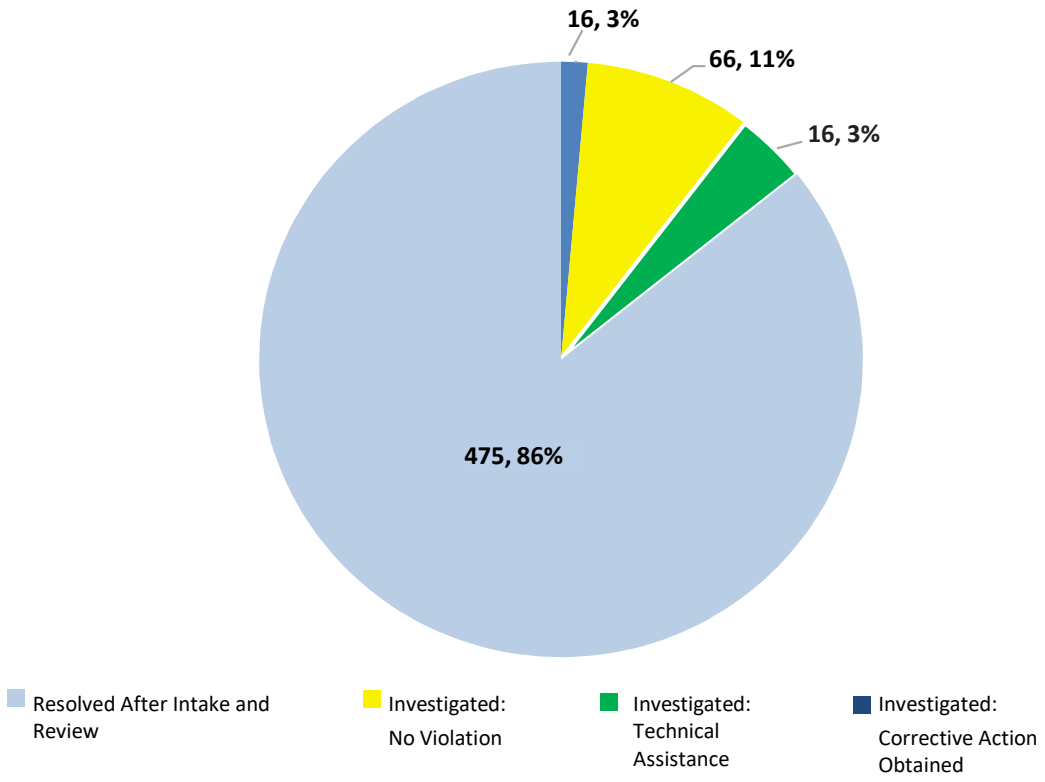

Figure 3

Subpoenas

OCR issued one subpoena in 2021.

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 2021 outreach highlights include:

- In 2021, OCR conducted 218 outreach events for HIPAA covered entities, business associates, and other health care industry stakeholders. Many of these virtual conferences focused specificallyon OCR actions related to the pandemic, including HIPAA enforcement discretion and guidance for telehealth.

- 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. Visits to OCR's HIPAA pages increased during the COVID-19 public health emergency, and the website averaged over 450,000 unique visits per month during 2021. OCR attributes this increase to the availability of HIPAA and COVID-19 guidance materials, and public interest in this content. For example, OCR's guidance on HIPAA, COVID-19 Vaccination, and the Workplace, issued on September 30, 2021, averaged more than 50,000 monthly visits for the remainder of the calendar year.

- In 2021, 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.

Audits

OCR did not initiate any audits in 2021 due to a lack of financial resources.

Appendix

Resolution Agreements[15] in 2021

Resolution Agreement with Banner Health

Banner Health (Banner) agreed to pay $200,000 and take corrective action to settle potential violations of the HIPAA Privacy Rule's right of access standard. Banner is a Phoenix, Arizona based not-for-profit organization that operates 30 hospitals and numerous primary care, urgent care, and specialty care facilities and is one of the largest health care systems in the United States.

OCR received two complaints filed against Banner entities alleging violations of the HIPAA right of access provisions. The first complaint alleged that the individual requested access to her medical records in December 2017 and did not receive the records until May 2018. The second complaint alleged that the individual requested access to an electronic copy of his records in July and September 2019 and the records were not sent until February 2020. OCR's investigations determined that Banner entities' failure to provide timely access to the requested medical records were potential violations of the HIPAA right of access standard. OCR initiated an investigation, and, as a result of OCR's intervention, the requested records were provided to the complainants. OCR's investigation found that Banner failed to provide the complainants with timely access to their PHI.

In addition to the monetary settlement, Banner agreed to:

- Revise its right of access policies and procedures to comply with the HIPAA Privacy Rule;
- Train workforce members on the revised policies and procedures and HIPAA's right of access provisions; and
- Certify that all workforce members that are involved in receiving or fulfilling access requests are trained on its revised policies and procedures and the HIPAA right of access provisions.

This settlement occurred in January 2021. The resolution agreement is available at the following link:
www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/banner/index.html.

[15] 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 2021.

Resolution Agreement with Excellus Health Plan

Excellus Health Plan (Excellus) agreed to pay $5,100,000 and take corrective action to settle potential violations of the HIPAA Privacy and Security Rules. Excellus is a New York health services corporation that provides health insurance coverage to over 1.5 million people in Upstate and Western New York.

OCR began investigating Excellus after it filed a breach report stating that cyber-attackers had gained unauthorized access to its information technology systems. The hackers installed malware and conducted reconnaissance activities that ultimately resulted in the impermissible disclosure of the PHI of more than 9.3 million individuals. OCR's investigation found potential violations of the HIPAA Rules including failure to conduct an enterprise-wide risk analysis, and failures to implement risk management, information system activity review, and access controls.

In addition to the monetary settlement, Excellus agreed to:

- Conduct a comprehensive and thorough risk analysis;
- Develop an enterprise-wide Risk Management Plan to address and mitigate any security risks and vulnerabilities found in the risk analysis; and
- Revise or develop policies and procedures to comply with the HIPAA Rules.

This settlement occurred in January 2021. The resolution agreement is available at the following link:
www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/excellus/index.html.

Resolution Agreement with Renown Health

Renown Health (Renown) agreed to pay $75,000 and take corrective action to settle a potential violation of the HIPAA Privacy Rule's right of access standard. Renown is a private not-for-profit health system in Nevada.

In February 2019, OCR received a complaint alleging that Renown failed to respond in a timely manner to a patient's request that an electronic copy of her PHI be sent to a third party. OCR's investigation determined that Renown's failure to provide timely access to the requested records was a potential violation of the HIPAA right of access standard. As a result of OCR's investigation, Renown provided access to all of the requested records.

In addition to the monetary settlement, Renown agreed to:

- Develop or revise right of access policies and procedures to comply with the HIPAA Privacy Rule;
- Train workforce members on the revised policies and procedures and HIPAA's right of access provisions; and
- Revise its Notice of Privacy Practices to accurately reflect and convey to the public steps that individuals must take when requesting access to PHI.

This settlement occurred in February 2021. The resolution agreement is available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/renown/index.html.

Resolution Agreement with Sharp Healthcare dba Sharp Rees-Stealy Medical Centers

Sharp Healthcare dba Sharp Rees-Stealy Medical Centers (SRMC) agreed to pay $70,000 to settle a potential violation of the HIPAA Privacy Rule's right of access standard. SRMC is located in California and provides health care through four acute-care hospitals, three specialty hospitals, three affiliated medical groups, and a health plan.

In June 2019, a complaint was filed with OCR alleging that SRMC failed to take timely action in response to a patient's records access request directing that an electronic copy of PHI in an electronic health record be sent to a third party. OCR provided SRMC with technical assistance on the HIPAA right of access requirements. In August 2019, OCR received a second complaint alleging that SRMC still had not responded to the patient's records access request. OCR initiated an investigation and determined that SRMC's failure to provide timely access to the requested medical records was a potential violation of the HIPAA right of access standard. As a result of OCR's investigation, SRMC provided access to the requested records.

In addition to the monetary settlement, SMRC agreed to:

- Develop or revise right of access policies and procedures to comply with the HIPAA Privacy Rule;
- Train workforce members on the policies and procedures and HIPAA's right of access provisions; and
- Certify that all workforce members that are involved in receiving or fulfilling access requests are trained on its revised policies and procedures and the HIPAA right of access provisions.

This settlement occurred in February 2021. The resolution agreement is available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/sharp/index.html.

Resolution Agreement with The Arbour dba Arbour Hospital

The Arbour dba Arbour Hospital (Arbour) agreed to pay $65,000 and implement a corrective action plan to settle a potential violation of the HIPAA Privacy Rule's right of access standard. Arbour is located in Massachusetts and provides behavioral health services.

In July 2019, a complaint was filed with OCR alleging that Arbour failed to take timely action in response to a patient's records access request made in May 2019. OCR provided Arbour with technical assistance on the HIPAA right of access requirements. Later, in July 2019, OCR received a second complaint alleging that Arbour still had not responded to the same patient's records access request. OCR initiated an investigation and determined that Arbour's failure to

provide timely access to the requested medical records was a potential violation of the HIPAA right of access standard. As a result of OCR's investigation, Arbour provided the patient with a copy of their requested records in November 2019, more than 5 months after the patient's request.

In addition to the monetary settlement, Arbour agreed to:

- Develop or revise right of access policies and procedures to comply with the HIPAA Privacy Rule;
- Train workforce members on the policies and procedures and HIPAA's right of access provisions; and
- Certify that all workforce members that are involved in receiving or fulfilling access requests are trained on its revised policies and procedures and the HIPAA right of access provisions.

This settlement occurred in March 2021. The resolution agreement is available at the following link: www.hhs.gov/about/news/2021/03/24/ocr-settles-seventeenth-investigation-in-hipaa-right-of-access-initiative.html.

Resolution Agreement with Village Plastic Surgery

Village Plastic Surgery (VPS) agreed to take corrective actions and pay $30,000 to settle a potential violation of the HIPAA Privacy Rule's right of access provision. VPS is located in New Jersey and provides cosmetic plastic surgery services.

In September 2019, a complaint was filed with OCR alleging that VPS failed to take timely action in response to a patient's records access request made in August 2019. OCR initiated an investigation and determined that VPS's failure to provide timely access to the requested medical records was a potential violation of the HIPAA right of access standard. As a result of OCR's investigation, VPS sent the patient their requested records.

In addition to the monetary settlement, VPS agreed to:

- Review and revise its right of access policies and procedures to comply with the HIPAA Privacy Rule;
- Train workforce members on the HIPAA's right of access provisions;
- Certify that all workforce members that are involved in receiving or fulfilling access requests are trained on its revised policies and procedures and the HIPAA right of access provisions; and
- Submit a listing of all requests for access to PHI every ninety (90) days for the duration of the CAP.

This settlement occurred in March 2021. The resolution agreement is available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/vps/index.html.

Resolution Agreement with Peachstate Health Management dba AEON Clinical Laboratories

Peachstate Health Management dba AEON Clinical Laboratories (Peachstate) agreed to pay $25,000 and take corrective action to settle potential violations of the HIPAA Security Rule.

In December 2017, OCR initiated a compliance review of Peachstate to determine its compliance with the HIPAA Privacy and Security Rules. Peachstate is based in Georgia and provides diagnostic and laboratory-developed tests, including clinical and genetic testing services. OCR's investigation found systemic noncompliance with the HIPAA Security Rule, including failures to conduct an enterprise-wide risk analysis, implement risk management and audit controls, and maintain documentation of HIPAA Security Rule policies and procedures.

In addition to the monetary settlement, Peachstate agreed to:

- Complete a comprehensive, enterprise-wide risk analysis;
- Develop a Risk Management Plan to address and mitigate any security risks and vulnerabilities found in the risk analysis;
- Develop, maintain, and revise, as necessary policies and procedures to comply with the HIPAA Rules; and
- Train all workforce members who have access to PHI on the HIPAA policies and procedures.

This settlement occurred in April 2021. The resolution agreement is available at the following link:
www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/peachstate/index.html.

Resolution Agreement with The Diabetes, Endocrinology &Lipidology Center

The Diabetes, Endocrinology & Lipidology Center (DELC), agreed to pay $5,000 and take corrective action to settle a potential violation of the HIPAA Privacy Rule's right of access provision. DELC is a West Virginia based healthcare providing treating Endocrine disorders.

OCR received a complaint alleging that DELC failed to take timely action in response to a parent's records access request for a copy of her child's PHI. OCR initiated an investigation and determined that DELC's failure to provide timely access to the requested medical records was a potential violation of the HIPAA right of access standard. As a result of OCR's investigation, DELC provided the requested records.

In addition to the monetary settlement, DELC agreed to:

- Review and revise its right of access policies and procedures to comply with the HIPAA Privacy Rule;
- Train all workforce members on the policies and procedures; and
- Submit a listing of all requests for access to PHI every ninety (90) days for the duration of the agreement.

This settlement occurred in April 2021. The resolution agreement is available at the following link: www.hhs.gov/about/news/2021/06/02/ocr-settles-nineteenth-investigation-hipaa-right-access-initiative.html.

Civil Money Penalty imposed on the Office of Dr. Robert Glaser

OCR imposed a civil money penalty of $100,000 against the Office of Dr. Robert Glaser for violations of the HIPAA Privacy Rule's right of access provision. Dr. Glaser is a solo practitioner based in New Hyde Park, New York specializing in cardiovascular diseases and disorders.

In November 2017, OCR received a complaint alleging that Dr. Glaser failed to respond to numerous written requests for medical records in 2013 and 2014. In December 2017, OCR closed the complaint after advising Dr. Glaser's office to provide the requested records if the requests met the requirements of the Privacy Rule. In March 2018, OCR received a second complaint from the complainant alleging that Dr. Glaser still had not provided him with a copy of his medical records. OCR initiated an investigation; however, Dr. Glaser's office did not respond to OCR's data requests or other inquiries regarding the investigation. Upon the conclusion of the investigation, OCR sent Dr. Glaser's office a notification of proposed determination notifying him of the results of the investigation and providing him with the opportunity to resolve the matter via a resolution agreement and corrective action plan. After receiving no response, OCR imposed a civil money penalty in the amount of $100,000.

The notice of final determination was issued in May 2021. The notice of proposed determination and notice of final determination are available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/glaser/index.html.

Civil Money Penalty imposed on U. Phillip Igbinadolor, D.M.D. & Associates

OCR imposed a civil money penalty of $50,000 against Dr. U. Phillip Igbinadolor, D.M.D. & Associates (UPI) for violation of the HIPAA Privacy Rule. UPI is a dental practice with offices in Charlotte and Monroe, North Carolina.

In November 2015, OCR received a complaint alleging that UPI had violated the HIPAA Privacy Rule by impermissibly disclosing PHI in social media review responses. OCR notified UPI of its investigation on July 21, 2016. OCR's investigation found that UPI impermissibly disclosed PHI on a webpage in response to a negative online review. UPI did not respond to OCR's data request, did not respond or object to an administrative subpoena, and waived its rights to a hearing by not contesting the findings in OCR's Notice of Proposed Determination. Subsequently, OCR imposed a $50,000 civil money penalty.

The notice of final determination was issued in June 2021. The notice of proposed determination and notice of final determination are available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/upi/index.html.

Resolution Agreement with Children's Hospital & Medical Center

Children's Hospital & Medical Center agreed to pay $80,000 and take corrective action to settle a potential violation of the HIPAA Privacy Rule's right of access standard. CHMC is located in Omaha, Nebraska, and provides pediatric health care services.

In May 2020, OCR received a complaint from a parent alleging that CHMC failed to provide the parent with a complete copy of their child's medical records despite numerous requests. OCR initiated an investigation and determined that CHMC's' failure to provide all requested medical records was a potential violation of the HIPAA right of access standard. As a result of OCR's investigation, CHMC provided a complete copy of the requested medical records.

In addition to the monetary settlement, CHMC agreed to:

- Review and revise right of access policies and procedures to comply with the HIPAA Privacy Rule;
- Train workforce members on policies and procedures; and
- Certify that all workforce members that are involved in receiving or fulfilling access requests are trained on its revised policies and procedures and the HIPAA right of access provisions.

This settlement occurred in August 2021. The resolution agreement is available at the following link: www.hhs.gov/about/news/2021/09/10/ocr-resolves-twentieth-investigation-in-hipaa-right-of-access-initiative-with-settlement.html.

Resolution Agreement with Denver Retina Center

Denver Retina Center (DRC) agreed to pay $30,000 and adopt a corrective action plan to settle a potential violation of the HIPAA Privacy Rule's right of access standard. DRC is a medical practice located in Denver, Colorado and provides ophthalmologic services to the surrounding community.

In June 2019, OCR received a complaint alleging that DRC failed to provide the complainant with her medical records after requesting them multiple times. OCR initiated an investigation and DRC provided evidence that it had provided the requested medical records. OCR's investigation determined that DRC failed to provide timely access to PHI and DRC did not have adequate Access policies and procedures in accordance with the HIPAA Privacy Rule.

In addition to the monetary settlement, DRC agreed to:

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

- Certify that all workforce members that are involved in receiving or fulfilling access requests are trained on its revised policies and procedures and the HIPAA right of access provisions.

This settlement occurred in August 2021. The resolution agreement is available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/denver-retina/index.html.

Resolution Agreement with Rainrock Treatment Center dba Monte Nido Rainrock

Rainrock Treatment Center dba Monte Nido Rainrock (Monte Nido) agreed to pay $160,000 and adopt a corrective action plan to settle a potential violation of the HIPAA Privacy Rule's right of access standard. Monte Nido is located in Miami, Florida, and provides behavioral health services.

In December 2019, January 2020, and February 2020, OCR received complaints alleging that Monte Nido failed to provide the complainant with a copy of her medical records after numerous requests. OCR initiated an investigation and determined that Monte Nido's failure to provide timely access to medical records was a potential violation of the HIPAA right of access standard. As a result of OCR's investigation, the complainant received a copy of her medical records.

In addition to the monetary settlement, Monte Nido agreed to:

- Develop or revise right of access policies and procedures to comply with the HIPAA Privacy Rule;
- Train workforce members on the policies and procedures; and
- Certify that all workforce members that are involved in receiving or fulfilling access requests are trained on its revised policies and procedures and the HIPAA right of access provisions.

This settlement occurred in August 2021. The resolution agreement is available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/monte-nido/index.html.

Resolution Agreement with Advanced Spine & Pain Management

Advanced Spine & Pain Management (ASPM) agreed to pay $32,150 and adopt a corrective action plan to settle a potential violation of HIPAA Privacy Rule's right of access standard. ASPM is a medical center located in Cincinnati, Ohio and provides treatment for the management and treatment chronic pain.

OCR received a complaint alleging that the complainant requested his PHI in writing but did not receive the requested information. OCR initiated an investigation and determined that ASPM's failure to provide timely access to medical records was a potential violation of the HIPAA right of access standard. As a result of OCR's investigation, ASPM sent the complainant a copy of his

medical records.

In addition to the monetary settlement, ASPM agreed to:

- Develop or revise right of access policies and procedures to comply with the HIPAA Privacy Rule;
- Train workforce members on policies and procedures; and
- Certify that all workforce members that are involved in receiving or fulfilling access requests are trained on its revised policies and procedures and the HIPAA right of access provisions.

This settlement occurred in September 2021. The resolution agreement is available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/aspm/index.html.

Resolution Agreement with Wake Health Medical Group

Wake Health Medical Group (WHMG) 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 standard. WHMG is located in Raleigh, North Carolina, and provides primary care and allied services.

In December 2020, OCR received a complaint alleging that WHMG failed to provide the complainant with a copy of her medical records after requesting them in June 2019 and paying a fee of $25 for the records. OCR's investigation determined that WHMG's failure to provide timely access to medical records was a potential violation of the HIPAA right of access standard. As a result of OCR's investigation, WHMG provided the complainant with a copy of her medical records.

In addition to the monetary settlement, WHMG agreed to:

- Review and revise, if necessary, its right of access policies and procedures to comply with the HIPAA Privacy Rule;
- Train all workforce members on the policies andprocedures; and
- Submit a listing of all requests for access to PHI every ninety (90) days.

This settlement occurred in October 2021. The resolution agreement is available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/wake-health/index.html.

Resolution Agreement with Jacob & Associates

Jacob & Associates (Jacob) agreed to pay $28,000 and adopt a corrective actionplan to settle a potential violation of the HIPAA Privacy Rule's right of access standard. Jacob is a health care

provider of psychiatric services with two locations in California.

In November 2018, OCR received a complaint alleging that Jacob failed to respond to an individual's multiple requests for 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. OCR also determined that the practice failed to provide access in the form and format requested, imposed an unreasonable fee, and failed to implement policies and procedures regarding the right of access. As a result of OCR's investigation, Jacob provided the individual with their requested medical records.

In addition to the monetary settlement, Jacob agreed to:

- Develop or revise right of access policies and procedures to comply with the HIPAA Privacy Rule;
- Train workforce members on HIPAA's right of access provisions;
- Certify that all workforce members that are involved in receiving or fulfilling access requests are trained on its revised policies and procedures and the HIPAA right of access provisions.

This settlement occurred in December 2021. The resolution agreement is available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/jacob-associates/index.html.

Settlement Agreement with Donald B. Brockley, D.M.D.

Donald B. Brockley, D.M.D., (DBB) agreed to pay $30,000 and take corrective actions to settle a potential violation of the HIPAA Privacy Rule's right of access standard. DBB is a solo dental practitioner located in Butler, Pennsylvania.

OCR received a complaint alleging that DBB failed to provide the complainant with a copy of her medical records. OCR initiated an investigation and determined that DBB's failure to provide the requested medical records was a potential violation of the HIPAA right of access standard. In August 2019, OCR informed DBB of the results of its investigation and its potential violations and provided DBB with an opportunity to submit written evidence of any mitigating factors or affirmative defenses to determine whether a civil money penalty should be imposed. In November 2020, OCR issued a notice of proposed determination and notified DBB that it was proposing a civil money penalty in the amount of $104,000. In January 2021, DBB requested a hearing before an Administrative Law Judge to contest the imposition of a civil money penalty. In October 2021, both parties filed for a stay in proceedings to resolve their dispute. A monetary settlement was reached.

In addition to the monetary settlement, DBB agreed to:

- Provide the Complainant with her entire designated record set;
- Develop right of access policies and procedures to comply with the HIPAA Privacy Rule; and
- Train workforce members on HIPAA's right of access provisions.

This settlement occurred in December 2021. The resolution agreement is available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/brockley/index.html.